IDA PAPER P-2783

AS-IS (ACTIVE SAFING AND ISOLATION SYSTEM):

A Satellite-Based Remote Continuing Authorization Concept with Application to Control of Naval Strategic Nuclear Missiles and Tactical Weapons

D. M. Nosenchuck
W. J. A. Dahm

June 1992

INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street, Alexandria, Virginia 22311-1772

DEFINITIONS

IDA publishes the following documents to report the results of its work.

Reports

Reports are the most authoritative and most carefully considered products IDA publishes. They normally embody results of major projects which (a) have a direct bearing on decisions affecting major programs, (b) address issues of significant concern to the Executive Branch, the Congress and/or the public, or (c) address issues that have significant economic implications. IDA Reports are reviewed by outside panels of experts to ensure their high quality and relevance to the problems studied, and they are released by the President of IDA.

Group Reports

Group Reports record the findings and results of IDA established working groups and panels composed of senior individuals addressing major issues which otherwise would be the subject of an IDA Report. IDA Group Reports are reviewed by the senior individuals responsible for the project and others as selected by IDA to ensure their high quality and relevance to the problems studied, and are released by the President of IDA.

Papers

Papers, also authoritative and carefully considered products of IDA, address studies that are narrower in scope than those covered in Reports. IDA Papers are reviewed to ensure that they meet the high standards expected of refereed papers in professional journals or formal Agency reports.

Documents

IDA Documents are used for the convenience of the sponsors or the analysts (a) to record substantive work done in quick reaction studies, (b) to record the proceedings of conferences and meetings, (c) to make available preliminary and tentative results of analyses, (d) to record data developed in the course of an investigation, or (e) to forward information that is essentially unanalyzed and unevaluated. The review of IDA Documents is suited to their content and intended use.

The work reported in this publication was conducted under IDA's Independent Research Program. Its publication does not imply endorsement by the Department of Defense, or any other Government agency, nor should the contents be construed as reflecting the official position of any Government agency.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 1992	Final

4. TITLE AND SUBTITLE

AS-IS (ACTIVE SAFING AND ISOLATION SYSTEM): A Satellite-Based Remote Continuing Authorization Concept with Application to Control of Naval Strategic Nuclear Missiles and Tactical Weapons

5. FUNDING NUMBERS

MDA 903 89 C 0003

CRP 9000-125

6. AUTHOR(S)

Daniel M. Nosenchuck and Werner J.A. Dahm

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street
Alexandria, VA 22311

8. PERFORMING ORGANIZATION REPORT NUMBER

IDA Paper P-2783

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Public release/unlimited distribution.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This paper describes a system for maintaining control of high technology weapons either before or after they have been launched. The system is applicable to weapons with either conventional or non-conventional warheads, and could be used both for the control of weapons of U.S. forces as well as those sold to other nations. The particular application considered in this paper is the control of U.S. naval strategic weapons. The system, called AS-IS (Active Safing and Isolation System), is based on globally transmitted messages, continuously sent by the National Command Authority (NCA) via one-way satellite links, to receiver modules embedded in the weapons and coupled to their on-board arming/guidance circuitry. In the event of a missile launch, the on-board AS-IS module receives the encrypted NCA signal at breakwater and reacts accordingly. In peacetime, 'DISABLE' signals would be broadcast continuously, causing any launched weapon to disarm and abort its flight. During periods of increased readiness, or in wartime, NCA would transmit 'ENABLE' signals either to selected weapons or to all weapons. The one-way nature of the message transmissions and the default 'ENABLE' feature in the event of any NCA signal disruption thus maintain the stealth aspects and launch autonomy of the submarine platform, while allowing NCA control over accidental/unauthorized SLBM launches in periods of reduced tension.

14. SUBJECT TERMS

Arms Control, Ballistic Missile Submarine (SSBN), Permissive Action Links (PALS), Submarine Launched Ballistic Missile (SLBM).

15. NUMBER OF PAGES

108

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAME AS REPORT

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

IDA PAPER P-2783

AS-IS (ACTIVE SAFING AND ISOLATION SYSTEM):

A Satellite-Based Remote Continuing Authorization Concept with Application to Control of Naval Strategic Nuclear Missiles and Tactical Weapons

D. M. Nosenchuck
W. J. A. Dahm

June 1992

INSTITUTE FOR DEFENSE ANALYSES
IDA Independent Research Program

PREFACE

This report, funded as an IDA Central Research Project, grew out of the authors' participation in the Defense Science Study Group (DSSG) organized by IDA. The DSSG is a program of education and study for young professors of science, engineering and mathematics who have achieved national recognition in their fields. The goal of the program is to foster a long-term interest in national security issues among the DSSG members through technical briefings by officials in government and specialists in defense and industry, and site visits to military, industrial and national laboratory facilities. During this program, the authors developed a new concept for the control of tactical weapons. Upon completion of the DSSG program, the authors continued their study under IDA sponsorship, expanding the concept to strategic weapon systems.

(This page intentionally left blank)

TABLE OF CONTENTS

Appendixes

LIST OF FIGURES

(This page is intentionally left blank)

GLOSSARY

AS-IS	Active Safing and Isolation System
BER	Bit-error rate
DSSG	Defense Science Study Group
ECC	Error-checking and correction
EM	Electromagnetic
EMI	Electromagnetic interference
EW	Electromagnetic Warfare
FARR	Failsafe and Risk Reduction Review
FISSS	Frequency-independent strong signal suppressor
FMA	Foreign military aid
FMS	Foreign military sales
GPS	Global Positioning System
MTBF	Mean time between failure
NCA	National Command Authority
PAL	Permissive-action link
RPAL	Remote permissive-action link
SAM	Surface-to-air missile
SLBM	Submarine launched ballistic missile
SLCM	Sea launched cruise missile
SNR	Signal/noise ratio

(This page is intentionally left blank)

I. INTRODUCTION

The principal objection against permissive-action links (PALs) in submarine-based strategic nuclear missiles has traditionally been that any requirement for a launch authorization message from an external National Command Authority (NCA) compromises the threat posed by an autonomous vehicle like the submarine. At present, even if all communications assets should fail in a conflict, or if the ground- and air-based legs of the strategic triad become incapacitated, the autonomous submarines would remain an extremely potent nuclear retaliatory threat. Submarine-based strategic nuclear missiles thus serve as a highly-effective final stabilizing element in the triad. However, to achieve this situation, the risk of an unauthorized or accidental missile launch becomes part of the equation.

Though the absence of PALs in submarine launched ballistic missiles (SLBMs) has long been a subject of some concern, the willingness to accept the risk that this situation poses has been significantly altered by geopolitical changes that have occurred over the past 2 years. This has become a topic of renewed discussion, and has recently been brought under formal review by the Kirkpatrick Failsafe and Risk Reduction Review (FARR) Committee, as well as the National Academy of Sciences Committee on International Security and Arms Control. Some form of protective measures for SLBMs may indeed be in the offing. Solutions thus need to be explored that effectively allow some form of control to be asserted over accidental or unauthorized SLBM launches during peacetime. However, it is essential that any options being considered must not compromise either the stealth characteristics of the submarine platform itself, or the launch autonomy that is central to the submarine's key stabilizing role in the strategic triad during both peace and war.

This report describes a new concept called AS-IS (Active Safing and Isolation System) for a satellite-based remote permissive-action link (RPAL) providing continual NCA control capability over advanced electronic systems. The major components of the AS-IS concept are quite general, and can be implemented in various ways for specific strategic, tactical, and commercial applications. In the configuration described here for SLBM use, AS-IS appears to provide a workable solution for the SLBM "authorization

problem," while at the same time satisfying traditional objections against the use of conventional PALs in submarine-based nuclear strategic missiles.

The AS-IS concept was originally developed [Ref. 1] during the IDA/DARPA Defense Science Study Group (DSSG) 1990 Summer Study, and focused primarily on implementations to allow control of large numbers of tactical weapons. A subsequent description [Ref. 2] introduced the application of AS-IS for control of SLBMs/sea launched cruise missiles (SLCMs). This IDA Central Research Project Final Report focuses primarily on the potential suitability of AS-IS as a solution for the SLBM PAL problem, allowing NCA to deal with accidental or unauthorized missile launches.[1] Additional applications are briefly summarized for various tactical weapon implementations, both for foreign military aid (FMA) and foreign military sales (FMS) units, as well as for certain commercial implementations in advanced consumer electronics.

A. GENERAL OVERVIEW OF AS-IS

In its simplest form, the AS-IS concept involves a small package of microelectronic receiver/amplifier/logic circuitry embedded on board a weapon, which reacts to a suite of globally transmitted action sequence messages to provide central remote control over the functional state of the weapon. The general idea is shown schematically in Figure 1. Messages are continuously transmitted by the NCA via secure one-way satellite links to AS-IS receiver units equipped with omnidirectional antennas. The AS-IS receivers are typically embedded deeply within the on-board arming/guidance circuitry of the weapon. A unique digital address assigned to each individual AS-IS receiver module allows the NCA to exercise enable/disable control, or even functional reprogrammability, over entire classes of weapons, over selected groups of weapons, or even over individual fielded weapons. Global coverage afforded by the AS-IS satellite link removes the need for any physical access to the weapon, or even the need for any knowledge of the weapon location. The AS-IS units are strictly passive receivers, and cannot disclose the presence of the weapon in which they are contained. The entire set of AS-IS module addresses required to assert control over large numbers of weapons can be cycled through in a very short time. If for any reason transmission of the AS-IS messages to the weapon is interrupted or terminated, the AS-IS unit automatically defaults to a predetermined state of functionality. If the integrity of the AS-IS unit itself is in any way compromised or fails, the weapon also enters

---

[1] The SLBM implementation described here reflects numerous inputs offered during summary briefings given to various agencies over the past 18 months.

this predetermined default functional state. AS-IS thus provides the capability for NCA to rapidly and reliably address individual weapons or groups of weapons - fielded in potentially unknown global locations - without any direct physical access, and alter or reprogram their functionality.

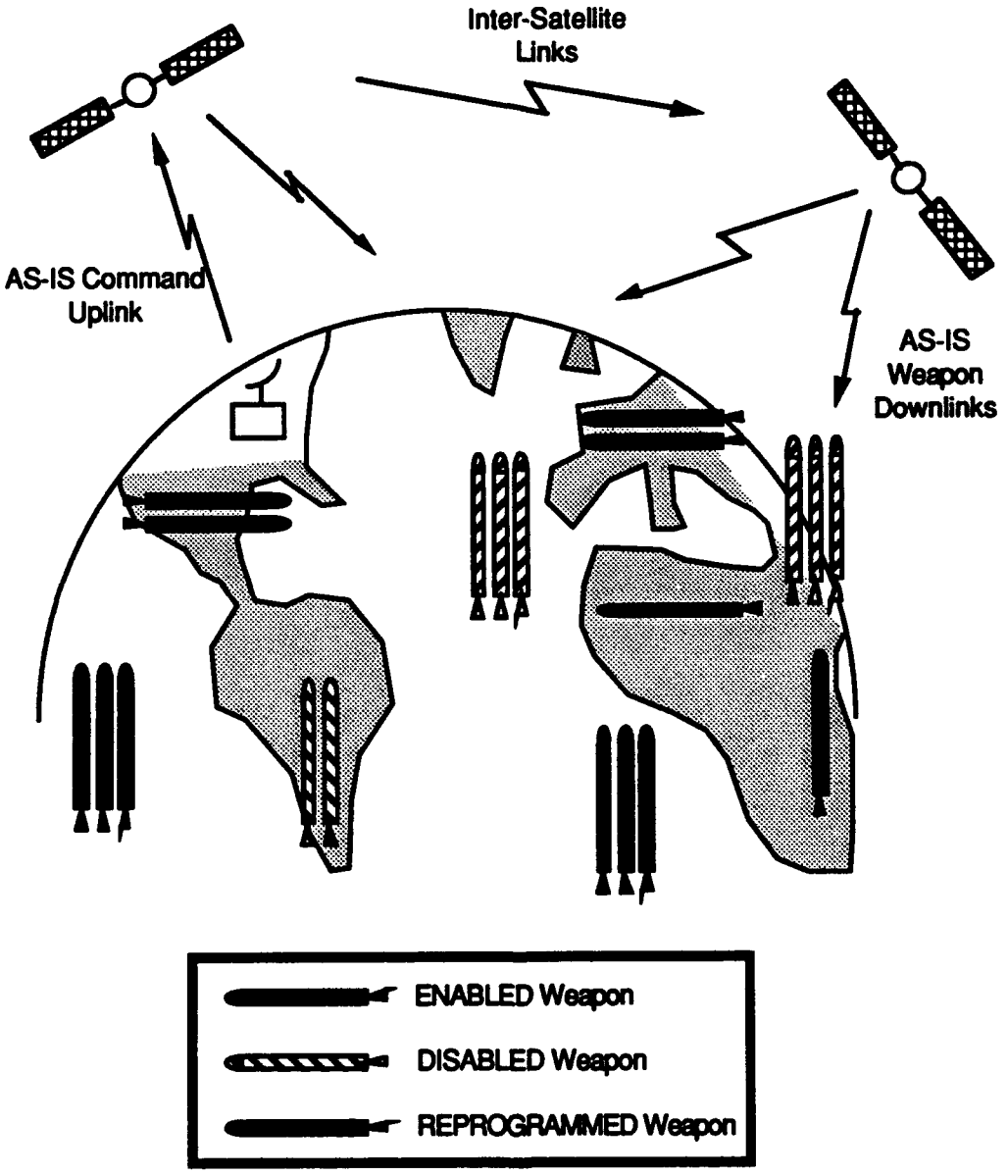


Figure 1. The Global AS-IS Concept for Continuing Authorization of Weapon Systems Through Satellite Links to Receiver Modules in Individual Fielded Weapons

B. AS-IS IMPLEMENTATION FOR SLBMS

The SLBM configuration of AS-IS is indicated schematically in Figure 2. In this case, the predetermined default state corresponds to an 'ENABLE' mode, in which full functionality of the weapon is available. In effect, the missile in this state is entirely unaffected by the presence of the AS-IS module. Since the NCA's UHF transmissions do not penetrate the oceans, missiles in their launch tubes continually remain in this default 'ENABLE' state. During peacetime, the NCA would continuously broadcast 'DISABLE' signals to all SLBM AS-IS addresses. In the event of a missile launch, the AS-IS unit on board the missile would first receive the encrypted NCA signal at breakwater, and react accordingly. When the NCA transmission directs the missile into its 'DISABLE' state, the launched SLBM disarms itself and aborts its flight by altering its trajectory and/or self-destructing. On the other hand, during periods of increased force readiness, or in wartime, NCA would broadcast 'ENABLE' signals to selected SLBMs, or to all missiles, allowing their full functionality just as though AS-IS were not present. Even if the NCA's ability to transmit the 'ENABLE' codes were compromised, interrupted, or terminated, the missile would still automatically default into the 'ENABLE' state and be fully functional. AS-IS thus never prevents launch of an SLBM. Moreover, successful action sequence is required only during peacetime to abort accidental or unauthorized missile launches.

C. AS-IS VS. CONVENTIONAL PALS

AS-IS, as summarized above for application to SLBMs, is in many ways the logical opposite of a traditional PAL. Unlike conventional physical-access PALs, AS-IS is a purely remote-access concept. More importantly, traditional PALs require a specific positive action sequence to permit functionality of the weapon. In contrast, AS-IS allows full weapon functionality in the absence of any action – a positive AS-IS action sequence is needed only if the weapon functionality is to be blocked. Conventional PAL concepts involve a weak link through an external launch authorization message from the NCA. AS-IS, on the other hand, allows launch even under a catastrophic failure of the NCA transmission link. AS-IS thus fully maintains the launch autonomy of the SLBM platform during wartime, which is key to the submarine's principal role in the strategic triad, as well as preserving the stealth characteristics of the submarine itself. At the same time, AS-IS effectively introduces a capability for NCA to assert control over accidental or unauthorized SLBM launches during peacetime or in lower states of force readiness.

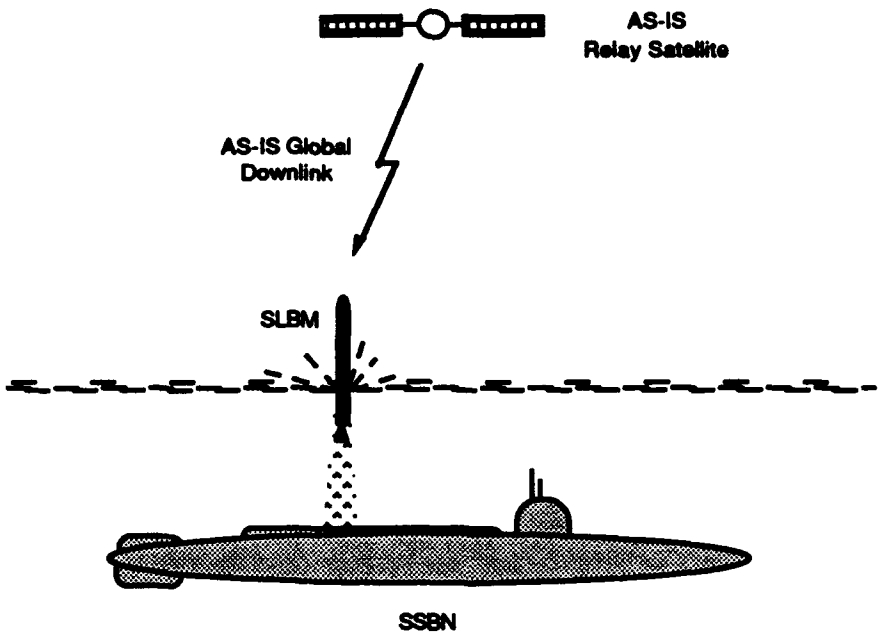


Figure 2. AS-IS Implementation for NCA Control Over Accidental/Unauthorized SLBM Launches During Peacetime

D. REPORT ORGANIZATION

This report is organized as follows. Section II introduces details of the general AS-IS concept and also describes a particular strawman implementation suitable for maintaining RPAL control over SSBN-launched strategic nuclear weapons. Section III discusses certain potential countermeasures to the SLBM implementation of AS-IS, and describes how various AS-IS features are meant to address them. Many of these countermeasure solutions are also applicable beyond the SLBM application. In fact, though AS-IS is currently being proposed primarily as a solution to the PAL problem for SLBMs/SLCMs, numerous other applications exist for which this concept provides unique capabilities, including both military and commercial scenarios. Some of these are discussed in Section IV. These include the implementation of AS-IS for control of tactical weapons, and offer novel capabilities for remote control over the functionality of certain classes of widely dispersed weapons often found in Third World countries as well as in terrorist arsenals. Section V summarizes some of the key points given here, and briefly discusses future directions in which the AS-IS concept development is progressing.

(This page is intentionally left blank)

II. THE AS-IS CONCEPT

AS-IS is a very general concept, providing for remote arm/disarm control or remote reprogrammability of high-threat tactical and strategic weapons, including both nuclear and non-nuclear as well as other nonconventional weapons. This section gives a description of various components of the AS-IS concept. For the purposes of concrete discussion, a specific strawman configuration of these components is given for the SLBM application described above. A technical assessment of the feasibility of these various embodiments is also included.

A. AS-IS COMMUNICATIONS LINK

Continuing authorization of weapons with installed AS-IS modules occurs over digital satellite links, which relay encrypted NCA messages from one or more transmission sites to weapons in the field. Uplink antennae are ground- and/or aircraft-based. A minimum of three geosynchronous satellites provide the primary AS-IS communications relay link for authorization commands, and are required for continuous global coverage within the relevant latitudes. Lower earth-orbit satellites, such as the existing 1.6 GHz Navstar Global Positioning System (GPS) satellites, might also be usable as a primary or secondary relay link, providing true global coverage.[1] The global satellite link obviates the need for any physical access to control the weapon, or even the need to know where the weapon is globally located. No knowledge of the location of either the weapon or the launch platform is required in order to address the AS-IS module.

A clock circuit internal to the AS-IS module enables the receiver and decoding electronics to detect and update the weapon status periodically[2] after a predetermined update time expires (e.g., once every few seconds). The AS-IS units are strictly receive-only – no response signals are broadcast from the weapon back to NCA, and no significant electromagnetic radiation is emitted from the electromagnetic interference (EMI)-shielded

---

1 Existing DSCS satellites, as well as the newer jam-resistant Milstar system, may be suitable for providing the primary AS-IS links.

2 This reduces the AS-IS module power requirement (see Section II.E). Alternatively, the AS-IS module can be configured in a listen-always mode independent of any internal clock.

module. The system is entirely passive and cannot electronically disclose the presence of the weapon or its launch platform. The message is received by the AS-IS module via a conformal antenna integrated into the weapon housing. A simple energy-per-bit analysis of the message integrity in the presence of noise allows an assessment of various communications link parameters. A single geosynchronous relay satellite is assumed in the field of view, with 10-50 watt transmitting power in the relevant AS-IS channel, directed into full hemisphere earth coverage. The typical receiver noise power is taken as $kT = 4 \times 10^{-21}$ J. To obtain a conservative estimate for the communication link integrity, a simple half-wave dipole antenna is assumed at the receiver.[3] The resulting ideal message signal/noise ratio (SNR) as a function of transmitter power, bandwidth, and carrier frequency is shown in Figure 3. Note that for many applications involving a relatively small number of AS-IS-equipped weapons and/or infrequent message repetition (such as in the SLBM problem), the system bandwidth can essentially be made arbitrarily small to yield acceptable levels of transmission integrity. Messages are continuously broadcast to all weapons on a list maintained by the NCA. The bandwidth is determined by the total number of AS-IS module addresses on this list and the desired message repetition period. A short repetition period permits rapid response, while a longer period allows for a lower system bandwidth. For n modules receiving L-bit packets, the system bandwidth bw is $bw = nL/T$ Hz, where T is the typical message repetition period in seconds. Of course, this repetition period need not be the same for all modules – it may be desirable to update some critical units more frequently than others.

As Figure 3 indicates, it is desirable to minimize the bandwidth requirements and carrier frequency to maximize the message integrity. At low SNR levels, a relatively large number of error-checking and correction (ECC) bits can be used to recover the message.[4] Link qualities of better than 10 dB appear achievable with carrier frequencies in the range of several hundred MHz to about 1 GHz (C-band), and for bandwidths up to about a MHz. For purposes of a conservative configuration, the strawman system will be assumed to consist of a 50 watt transmitter operating at 1 GHz with a 125-kHZ bandwidth. Lower carrier frequencies and potentially narrower bandwidths can produce better than 20 dB

---

3 A phased array receiver antenna [Ref. 3] may provide for higher link integrities, but the requisite signal processing may be excessive for many AS-IS applications.

4 Moreover, in a default 'ENABLE' implementation like the SLBM, it may not be essential to recover every valid transmission - only one valid 'DISABLE' transmission relatively early in the missile flight is needed accomplish the abort task.

signal quality with lower power transmitters. For the SLBM application, acceptable configurations exist with better than 50 dB link integrity.

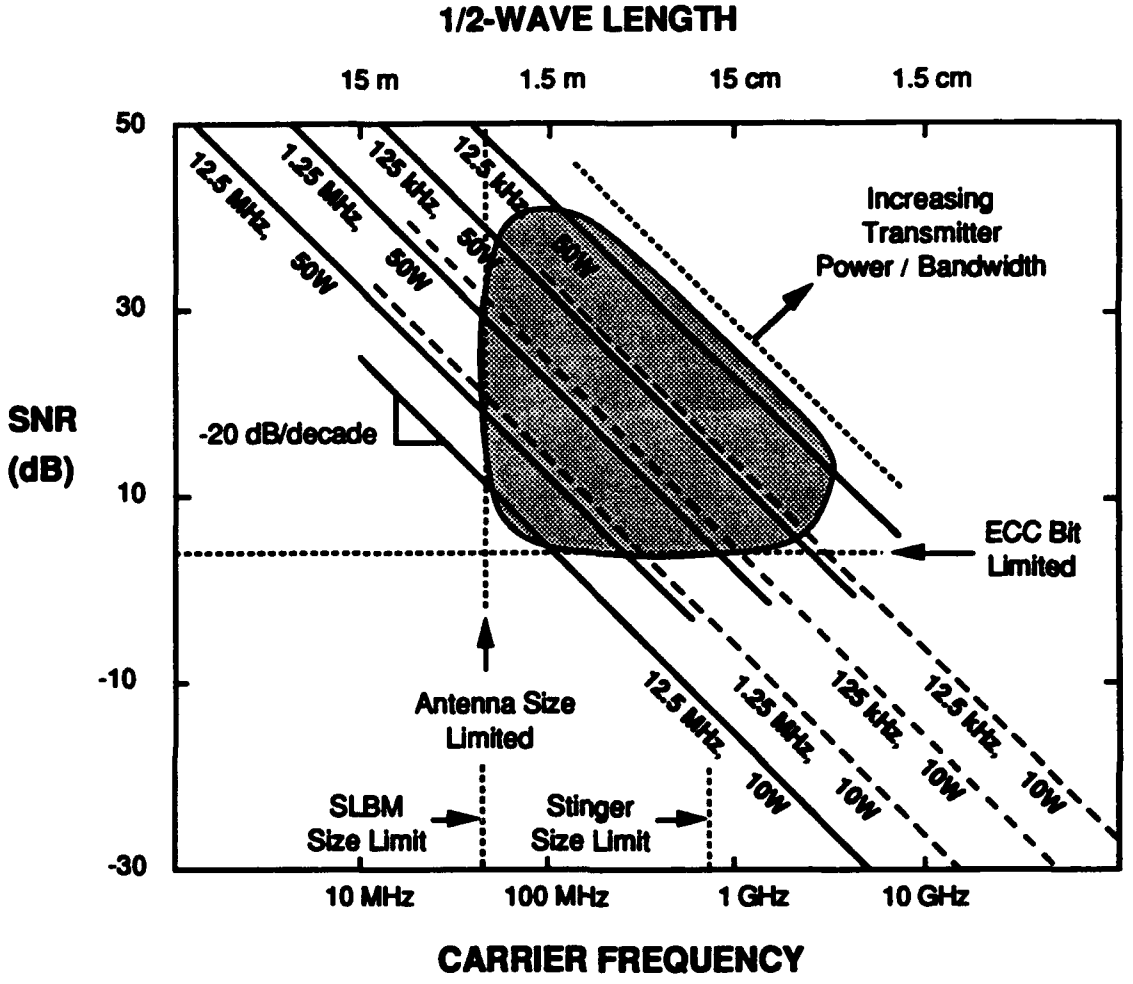


Figure 3. Schematic Indicating Ideal Signal-to-Noise Ratio (dB) Achievable With a Simple 1/2-Wave Dipole Antenna as a Function of Carrier Frequency, Transmission Bandwidth, and Transmitter Power for a Satellite Transmitter With Full Hemisphere Projected Coverage

Weapons on the NCA's transmission list are addressed in random sequences. This provides for increased security and also ensures that on average, each module will detect its address halfway through the message period. The latter decreases the AS-IS power requirements (see Section II.E) by approximately a factor of two, since the AS-IS receiver and amplifier are only enabled up to the time when the local unit is addressed. The NCA's

list can be reconfigured at will. In the strawman configuration 5,000 fielded weapons[5] can be continuously supervised if all their AS-IS modules were to be typically addressed once every 10 seconds; over 50,000 weapons can be controlled on a 2-minute cycle. More weapons could be controlled if the aggregate message repetition period is increased, while still maintaining the short repetition period for critical strategic weapons such as the SLBMs. In addition to discretely addressing individual AS-IS modules (e.g., a particular SLBM on a particular submarine launch platform), a hierarchical address structure allows NCA to assert enable/disable/reprogram control over groups of modules having common address fragments. Broadcast of a single command can then control, for example, all missiles on a certain submarine launch platform, or all missiles aboard a given group of submarines.[6]

Transmission over the satellite link occurs via secure one-way communication from NCA to the AS-IS receiver. The encrypted message structure is described in Section II.B. Message encryption occurs at the NCA; decryption occurs in the AS-IS module on-board the weapon. Several implementations of time-encoded, moving-lock, future-key encryption/decryption systems appear capable of maintaining message integrity and providing for secure message transmission. A strawman encryption/decryption scheme of this type, compatible with other aspects of the AS-IS system described here, is presented in Section II.C.

B. AS-IS MESSAGE FORMAT

For purposes of discussion, the length of the AS-IS message in the present strawman system is 256 bits. These are comprised of 192 data bits and 64 parity, ECC and reserved bits.[7] The 192 data bits, which comprise the remainder of the AS-IS message, provide for up to 2^{192} (more than 6×10^{57}) unique AS-IS module digital address codes. The majority of this data field is reserved for the missile address. The remainder is the action sequence and subsequent decryption information. Each AS-IS module decrypts the incoming 256-bit message packets, and compares the decrypted address to the local module

---

5 This number is about an order of magnitude larger than the current total number of SLBMs, consisting of roughly 150 Poseidon C-3s, 400 Trident 1 C-4s, and 100 Trident 2 D-5s.

6 Implementation of 'UNIVERSAL-DISABLE' and 'UNIVERSAL-ENABLE' codes, recognized by all modules, would allow further reduction in the system bandwidth requirements (with attendant improvements in message integrity) during nominal peacetime or wartime operations.

7 The 64 parity, ECC, and reserved bits are adequate to recover the true AS-IS message under conditions of relatively poor transmission integrity (see Section II.A)

address. If a match occurs, the non-address portion of the 192-bit data field is then decrypted to ascertain authorization, obtain future decryption key information, and determine the desired weapon action sequence.

In the simplest implementations, the AS-IS action sequence information would be comprised of a single bit, allowing 'ENABLE/DISABLE' actions only. This capability would be adequate for the SLBM application. During peacetime, or in appropriately low states of force readiness, the action sequence bit would be continually set to 'DISABLE', causing any launched missile to disarm itself and terminate its flight. In higher states of readiness, the action sequence bit can be set to 'ENABLE' for all SLBM addresses or for any subset of missiles, including individual SLBMs. Additional capabilities can be made available through additional action sequence bits. For example, a second bit could be set to select from a 'DESTRUCT/ABORT' option. After disarming itself in response to the first bit, the missile could then be made to either self-destruct, or to merely abort its trajectory. Depending on the level of functionality desired for any given application, the particular action sequence could be selected from any of a whole menu of options – just 8 bits in the action sequence fragment of the AS-IS message allows for 256 different actions to be offered.

Aside from the address and action sequence bits, the remainder of the 192 data bits contain the future decryption key information. Details of the moving-lock, future-key encryption/decryption system are given in Section C below.

C. AS-IS ENCRYPTION/DECRYPTION SCHEME

It is desirable to provide a robust, flexible operational environment where AS-IS-protected weapons do not have to continually listen to, or handshake with, the NCA. Weapon storage and transportation should not be subject to a requirement of receiving external messages. A simplistic way of achieving this would be to continually broadcast messages whose encryption key and format remain constant. A weapon with a factory-installed decryption key would then be able to successfully decipher the message at arbitrary times. However, there are several drawbacks to this simple approach, two of which are serious. The first is that an entire stream of messages could be passively recorded at any location, using a simple receiver and broad-band tape recorder. At a later date, the message stream could then be played back in the vicinity of the weapon in an electromagnetic (EM) shielded environment, which will generate a guaranteed weapon action based on the status of the message at the time of recording. A second problem is that

repetitive broadcast of a short (e.g., 256-bit) constant message provides more opportunity to compromise or fully breach message security.

To avoid these problems, yet maintain flexible receiver operations, a variable, time-sensitive, encryption/decryption scheme is proposed. The key required to decode messages on board the AS-IS module is comprised of two halves, somewhat analogous to public/private-key systems. One portion of the key is factory-installed in the AS-IS module. The remainder of the key, together with a short field containing the encrypted current time, is transmitted along with the authorization message to the remote AS-IS-equipped weapon. The AS-IS module decrypts the new message with an old decryption key, received at some prior time, as discussed below. The current message is then parsed for fields that delineate the new decryption key, new soft unit-address, weapon-authorization and status commands, and the current time. The received message is considered to be valid if the fields are properly formatted, and the difference between the received time-field and an on-board clock is within a prescribed tolerance. If the temporal error is too large, it is presumed that an 'old' message was received, and the weapon will enter its default state.

The new key will be used to decrypt the next message. Since message receipt occurs unpredictably, the key remains valid up to the next transmission. Once used, it is deleted and replaced by the new key. The remotely transmitted key is a member of an undepletable set of valid keys.[8] Once a key is used, it is deleted from that set. Thus, even though the encryption of messages may change on a cycle-by-cycle basis (e.g., every 2 minutes), a valid key can successfully decode the message the next time the AS-IS module begins listening, even though that time is non-deterministic from a system perspective and multiple keys may have been issued in the interim.

The address portion of the message format can be identified in the incoming signal without excessive difficulty. A code-breaking effort is therefore likely to start with that particular bit-field. To make that activity significantly more difficult, non-stationary 'soft' virtual-addresses are used. These virtual addresses are non-unique in that they can be mathematically transformed into a single logical address. This allows the address field to be variable, yet not time sensitive. Internal to an AS-IS module, the complete unit address is formed by combining the virtual field, encrypted and transmitted by the NCA, with a

---

[8] The ratio of invalid to valid keys can be made practically infinite, while still keeping the number of valid keys essentially infinite (see Section II.C).

factory-installed 'hard' address held within non-volatile AS-IS registers. The virtual addresses that are received are continually decrypted, transformed, and compared to the current address. If a match occurs (and the time-field is within error-bounds), the message is subsequently decoded and acted upon, along with updating the decryption key.

D. AS-IS DEFAULT FUNCTIONALITY

If a valid AS-IS message is not received by the module within a prescribed update time, the module defaults into a predetermined state. In the case of SLBMs, this default would be the 'ENABLE' state. In this 'ENABLE' state, the missile functionality is entirely the same as if the AS-IS module were not present in the weapon. Consequently, if the NCA transmissions are interrupted or terminated for any reason, or if the satellite link is in any way compromised (e.g., through failure of the NCA satellite link, jamming of the AS-IS channel, etc.), autonomous control of the weapon is returned to the submarine to permit its full functional use.

Typically, RF transmissions do not penetrate the seas to any useful depth. Thus AS-IS-equipped SLBMs on board a submerged launch platform would not receive any NCA messages, and would therefore constantly be in the default 'ENABLE' state. The presence of AS-IS aboard submarine-based missiles at sea does not interfere with the ability to launch the weapons. In the event of a missile launch, the first opportunity for AS-IS message receipt occurs immediately on breakwater.[9] Upon receipt of a valid message, the AS-IS module reacts accordingly. In peacetime, 'DISABLE' signals would presumably be broadcast continuously, causing any accidental or unauthorized launch of a weapon to be terminated via the missile entering a preset disable sequence, in which it disarms and aborts its flight by altering its trajectory and/or self-destructing. On the other hand, during various states of readiness, or in wartime, 'ENABLE' signals would be transmitted either to selected groups of weapons or to all weapons. In the 'ENABLE' state the missile functionality is entirely unaffected by the presence of the AS-IS module. Should the NCA transmissions fail to reach the module for any reason, the weapon simply defaults into the 'ENABLE' state and remains fully functional. AS-IS thus effectively prevents unauthorized/accidental missile launches during peacetime, while its default

---

9 For the minimum 1-second address cycle period needed to control all current SLBMs with the system configuration described in Section II.A, the AS-IS module would typically receive the encrypted NCA signal before the missile tail leaves the water.

'ENABLE' capability fully maintains the autonomy and stealth characteristics of the submarine platform during both peace and war.

E. AS-IS RECEIVER MODULE ELECTRONICS

The AS-IS module electronics are comprised of a receiver, an amplifier unit, a decryption processor, and an action sequence logic unit.[10] The complete module is compact, occupying roughly 10 cubic inches. In a typical application, the module electronics themselves might be physically distributed and deeply integrated into the guidance and fire-control circuitry, even collocated in the same circuit dies,[11] so that the entire weapon would be rendered inoperative by any attempt to remove the AS-IS electronics. Alternatively, a separate, hermetic, monolithic AS-IS receiver module could also be made virtually tamper-proof. Environmental sensors could be implemented in applications such as SLBMs, so that tampering generates a destruct current pulse that permanently disables the functionality of the weapon, or permanently sets the weapon into its default state.

The AS-IS module requires roughly 10 watt operating power during listen mode, and approximately 50 mW in standby. Power is supplied either by the host weapon or from a separate lithium battery housed together with the AS-IS module. Associated with the hardware module is an omnidirectional antenna. The antenna itself is compact and inexpensive, and could be implemented with conformal microstrip technology [Ref. 3] and integrated into the missile housing. Signal processing electronics to perform decryption are housed within the AS-IS module on board the missile itself.

At a minimum, AS-IS module reliability can be expected to be similar to other electronic mil-spec circuitry with comparable levels of functionality. Based on a very approximate gate count for the AS-IS module, the mean time between failure (MTBF) can be projected to lie in the range of 50 – 500 years. Although this likely exceeds the operational lifetime of the weapon, the hardware and electrical support systems, including leads, contacts, antenna, etc., often prove to be the more critical factor in determining the overall MTBF. A realistic assessment of the reliability and MTBF of these components remains to be performed.

---

10 A proof-of-concept module, having most of the key AS-IS concept functionalities, has been built for demonstration purposes and is described in Section II.F.

11 In the SLBM application, as well as in other retrofit applications, AS-IS modules would presumably be placed into existing missile hardware, precluding such deep physical integration with other on-board electronics. The nature of the SLBM, however, makes this level of integration less crucial.

F. AS-IS DEMONSTRATION PROTOTYPES

To illustrate the operational features of AS-IS, a simple hardware demonstrator was designed and fabricated. This system is comprised of: (1) an electronic unit that simulates the key relevant functions of the NCA message format and transmit-uplink facility, (2) a physically separate electronic unit that simulates the key satellite functions (receive/decode/shift/encode/transmit), and (3) two AS-IS receiver modules. The message is transmitted optically over a line-of-sight, pulse-width modulated, infrared carrier. The message length is short – 16 bits – with simple encryption selectable. The satellite accepts the encrypted uplink, decrypts, and re-encrypts the downlink. The transmitter and receiver layouts are shown roughly to scale in Figures 4 and 5.

The transmitter sends 'ABLE/DISABLE' commands to two independent AS-IS units. The messages may be sent either 'plain-text' or in encrypted form, and a 'UNIVERSAL-DISABLE' feature is included to over-ride the current messages and disarm all AS-IS units with a single action. Each receiver detects and decrypts, if appropriate, the AS-IS message-stream. When the unit address is detected, the 'ABLE/DISABLE' action code then updates the local module status. An 'arm/fire' button and 'weapon-away' light are used to simulate the key elements of an actual firing sequence. If the AS-IS module is in the 'ENABLE' state, the weapon-away light will illuminate when the fire-button arms and launches the 'weapon'. Otherwise, the light remains off. If a module does not receive a valid 'NCA' message within 10 seconds of a previous valid message, a 'fail-safe' indicator light will announce that the unit has entered its default state. In these demonstration units, which are meant to simulate the implementation of AS-IS in tactical weapons,[12] the default state is set to 'DISABLE'. In this state the weapon is incapable of being 'armed'. The AS-IS receiver will remain in the default state for a minimum period of 15 seconds, after which time receipt of a valid NCA message will bring it out of the default state. A 'status lock' button and indicator are used to illustrate a tactical operational mode of AS-IS, where a current status may be locked in and maintained, independent of external messages. This is demonstrated by remotely sending an 'ENABLE' command to either (or both) of the AS-IS receivers, then locking status on the receiver, and subsequently failing to send a valid message (typically achieved by blocking the infrared carrier). During the status-lock period (20 seconds), it is demonstrated that the 'weapon' can be 'armed' and 'fired' at will.

---

[12] See Section II.A.2 for additional AS-IS functionalities appropriate for tactical weapons *implementations.*

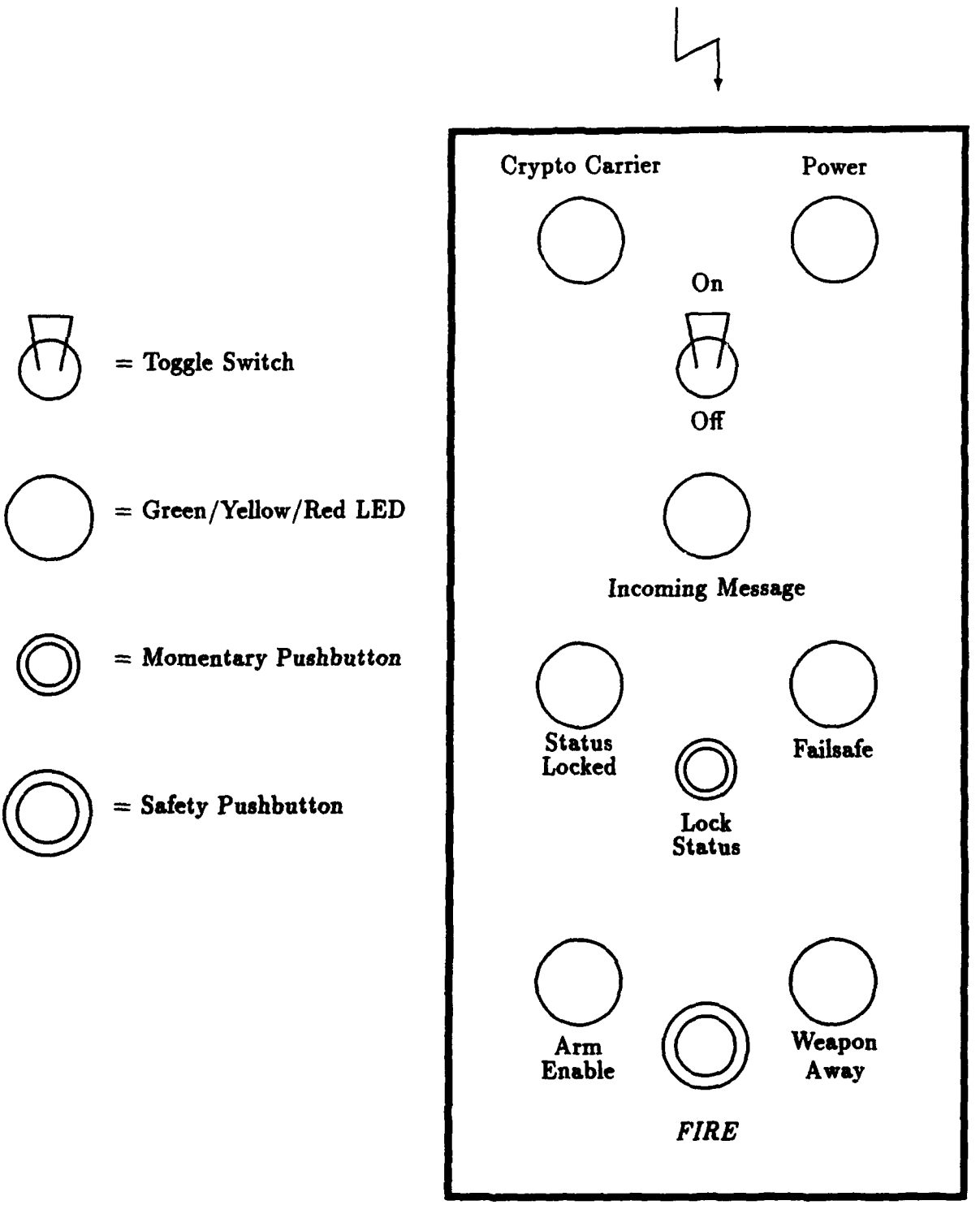


Figure 4. AS-IS Demonstration Receiver Layout

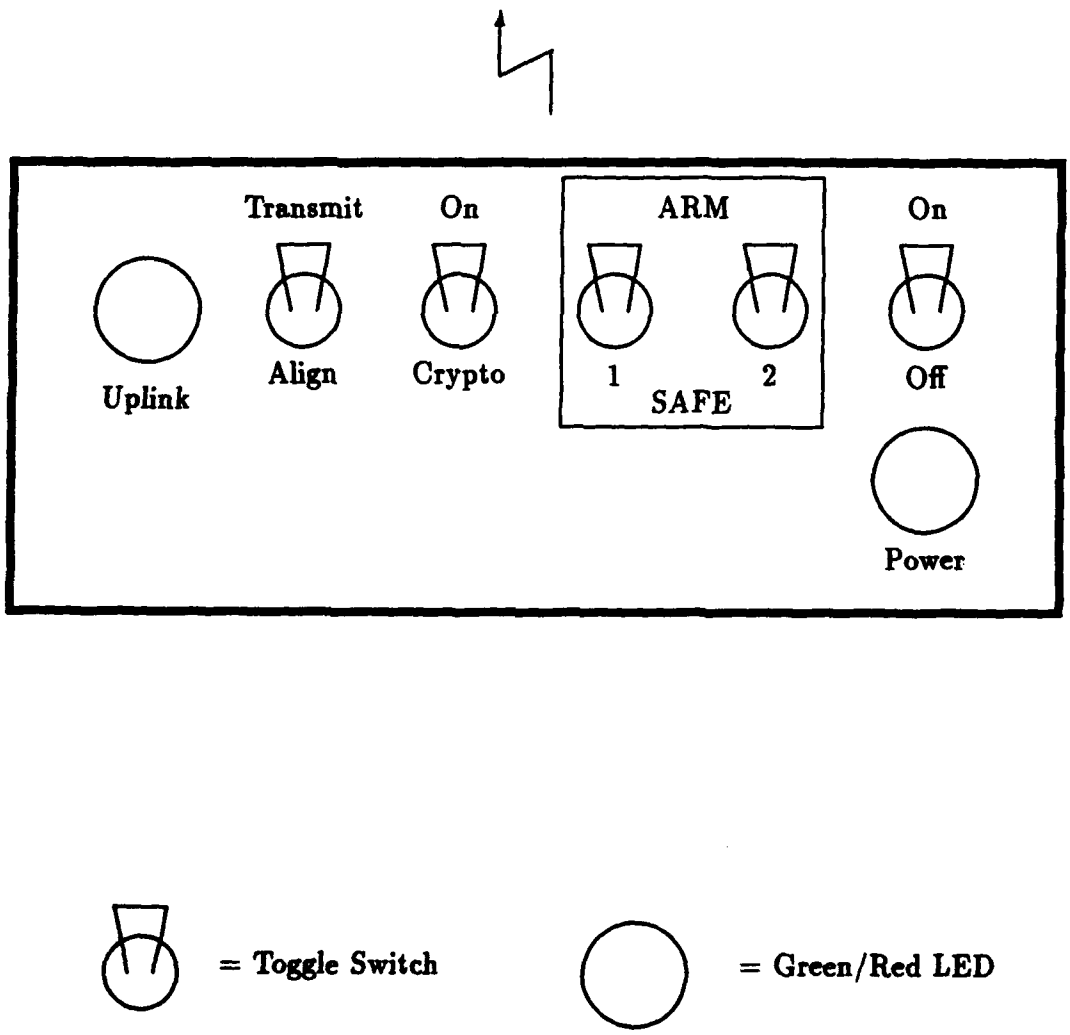


Figure 5. AS-IS Demonstration Transmitter Layout

However, once the status-lock period expires, the weapon automatically enters its default state unless or until a valid message permitting the weapon to be armed is received.

The four AS-IS demonstration modules (transmitter, satellite, and two receivers) are battery powered, fully portable, and fit in a small briefcase. The demonstration is generally run on a table top with 1-3 meters separation between the transmitter, satellite, and receivers. The uplink (transmitter-to-satellite channel) is optically bore-sighted to simulate the directional character of this link, while the downlink (satellite relay to multiple 'ground-based' units) is wide-field.

III. COUNTERMEASURES

The following section examines certain approaches that might be used as countermeasures against the AS-IS concept described above. This is not meant to be an exhaustive discussion of countermeasure possibilities, but to describe how various AS-IS features are meant to defeat some typical measures. Owing to the logical differences between AS-IS and conventional PALs, countermeasures for this type of system differ somewhat from those traditionally considered. In the simplest SLBM implementation, at any given time the NCA is broadcasting either the 'DISABLE' code or the 'ENABLE' code, and a given weapon is initially either in its appropriate NCA-directed state or in its default 'ENABLE' state.[1] It is useful to organize potential countermeasures along these distinctions. Similar classifications can be made for various tactical implementations, and many of the same counter-countermeasures discussed below also apply to those cases. Additional AS-IS features that become relevant for dealing with potential countermeasures in various tactical applications are discussed in Section IV.A.2.

A. FORCING AS-IS INTO THE 'ENABLE' STATE

In this situation, NCA is broadcasting 'DISABLE' codes, as would typically be the case during peacetime. The objective then would presumably be to keep one or more weapons in the 'ENABLE' state after launch to permit an unauthorized peacetime missile flight.[2] The weapon can be kept in this state quite readily simply by interrupting the NCA transmission link, thereby engaging the default 'ENABLE' state of the AS-IS unit. Any of numerous means for interrupting transmissions from the NCA site, or at the AS-IS relay satellites, can be effectively removed by a sufficiently redundant and distributed network of transmission sites and relay satellites. At the missile, actions aimed at incapacitating the

---

1 The default 'DISABLE' state is not relevant to the SLBM application, as described in Section II.E. However, this default mode becomes applicable to certain tactical weapon implementations of the AS-IS concept, and generates an entirely different set of countermeasure approaches. Some of these, in turn, create a need for various specialized AS-IS features, such as a current-state lock-in period, not applicable to the SLBM implementation. These are discussed in Section IV.A.2.

2 SLBMs equipped with AS-IS are continually in their default 'ENABLE' state when in their launch tubes, and thus AS-IS always permits an SLBM to be launched. The NCA 'DISABLE' transmissions during peacetime only interrupt the missile's flight after breakwater.

internal AS-IS circuitry within the housing to drive it into the default state would generally require physical access to the missile interior.[3] Attempts to sever the internal connections between the AS-IS antenna (integrated into the missile housing) and the primary AS-IS circuitry from outside the missile would typically require extremely high EM or current pulses.[4] These would presumably need to be applied while the missile is in its launch tube. Another approach would be to simply EM-shield the integrated AS-IS antenna to block message reception. Such a Faraday shield, installed while the missile is in its launch tube, would need to maintain its integrity throughout the missile ejection process and during the flight to be effective. Finally, it must be kept in mind that any successful action whatsoever to drive the weapon into the 'ENABLE' state accomplishes nothing more than placing one or more SLBM(s) into precisely the same state of risk that all SLBMs are presently in today.

B. FORCING AS-IS INTO THE 'DISABLE' STATE

This situation arises when NCA is broadcasting 'ENABLE' codes, during wartime or in various states of higher readiness, and the aim is to disable one or more missiles by driving it into the 'DISABLE' state. In this case, any measures that are 'destructive' from a systems perspective would be unproductive, since they only drive the weapon(s) into the default (i.e.,'ENABLE') state. Accordingly, similar countermeasures also become relevant when the weapon is initially in the default 'ENABLE' state. A large set of such countermeasures is centered around local (or even global) broadcast of false NCA 'DISABLE' transmissions to gain control of the AS-IS channel into one or more modules. Such approaches typically involve decryption of the AS-IS messages (see Section III.C below). Another method involves playing back earlier-recorded valid NCA 'DISABLE' transmissions (see Section III.D below).

C. AS-IS DECRYPTION COUNTERMEASURES

Attempts at illegitimate control of the AS-IS module by transmitting sequential or random permutations of all available 256-bit message codes can be neglected; the ratio of invalid to valid codes can be made sufficiently large to render this approach asymptotically

---

[3] These can be further diminished by a sufficiently deep integration of the AS-IS circuitry with other critical electronics on board the missile.

[4] In principle, this antenna link potentially provides an exposure of critical internal missile electronics to destructive EMP bursts in wartime that needed to be addressed (e.g., through a weak sacrificial antenna link).

futile.[5] Among genuine decryption efforts, code-breaking is likely to start with the address bit-field portion of the AS-IS message format (see Section II.B), since this fragment can be identified most readily in the NCA transmissions. To add significant difficulty to that activity, nonstationary virtual addresses can be used. This is distinct from the notion of changing decryption keys, in that the roving virtual address does not directly map to the physical address: it merely establishes a valid domain that the AS-IS module then uses. The physical AS-IS unit-address is factory-coded and held only within the tamperproof electronics module. Continually changing virtual addresses are relayed to the unit, decrypted, and compared to the current virtual address. If a match occurs, a virtual address space is created and the physical address is mapped to that space. If the physical address lies within that space, the action sequence portion of the message is subsequently decoded and acted upon, along with the storage of an updated virtual address and decryption key. The purpose of multilevel address decoding and maintenance of virtual/physical addresses is to ensure that a high level of message security is maintained.

D. AS-IS MESSAGE PLAYBACK COUNTERMEASURES

Another countermeasure to deal with the encrypted messages is to record NCA's 'DISABLE' broadcasts during peacetime and continually play them back to weapons stored in a shielded environment.[6] To deal with this situation, and to complicate code-breaking activities, a moving decryption key is proposed. The key required to decode messages on board the AS-IS module is comprised of two halves, somewhat analogous to public/private-key systems. One portion of the key is factory-installed in the AS-IS module, and the remainder is transmitted along with the authorization message to the module. The new key is used to decrypt the next message. Since message receipt occurs unpredictably,[7] the key remains valid up to the next valid transmission. After use, it is replaced by the new key. The remotely transmitted key is a member of a set of valid keys, and is deleted from that set once used. The set of valid keys can be made genuinely undepletable, while still keeping the ratio of invalid to valid keys essentially infinite (see footnote 18). Thus, even though the encryption of messages changes on a cycle-by-cycle

---

5 For example, if AS-IS is ultimately deployed in 10^6 weapons, more than 10^{70} invalid codes could be made to exist for each valid message sequence, based on a full 256-bit field. To put this in perspective, such a brute force decryption effort, operating continuously at the 125 kHz AS-IS bit frequency, would on average require more than 10 billion times longer than the age of the universe to stumble onto the correct AS-IS bit sequence for a particular weapon.

6 The digital storage required by such a system is not great, requiring less than 200 MBytes.

7 SLBMs typically will not begin to received the AS-IS transmissions until after breakwater.

basis, a valid key can successfully decode the message the next time the AS-IS module receives a transmission, even though multiple keys have been issued in the interim.

E. AS-IS MESSAGE JAMMING

Electronic interference or deliberate jamming often occurs in hostile environments. In the context of AS-IS, this could involve either uplink jamming directed at the relay satellites, or downlink jamming directed at the weapon(s). In both cases, the effect is to temporarily interrupt the NCA transmissions, thereby driving the AS-IS module into its default state. In the SLBM application, the default 'ENABLE' state makes jamming aimed at prohibiting missile launch during wartime useless. Jamming is thus relevant only during peacetime or in lower levels of force alert, when NCA is transmitting 'DISABLE' codes. In this situation, jamming must be maintained throughout the entire missile flight to block the module from receiving the NCA's 'DISABLE' transmission. Such jamming is easily detectable, and its effects can be practically removed through a distributed and redundant transmission and relay network. Moreover, as noted in Section III.A, any successful jamming effort under this scenario would only have the effect of leaving NCA without direct control over the SLBMs, just as is the case today.

Jamming appears not to be an issue in the SLBM application; however, in various tactical implementations of AS-IS (see Section III.B) this is not the case. Such applications typically involve a default 'DISABLE' state. To suppress the effects of jamming, techniques such as filtering, phase cancellation, directional antennae, or complex digital signal processing are often invoked singly or in combination. While many of these methods are effective to various degrees, they are often slow, cumbersome to implement, mission-limiting, and/or costly. Although a complete treatment of suppression techniques is beyond the present scope, several remarks can be made relative to a new system that warrants consideration for AS-IS jamming suppression.

A system that reduces the adverse effects of strong-amplitude interference[8] has been recently studied [4]. The frequency-independent strong signal suppressor (FISSS) uses a simple nonlinear-load element in a filter-type circuit. Analogous to frequency-domain filtering, the circuit's transfer characteristics are based on input amplitude. Large amplitude

[8] If signals are present that are near or below the anticipated level of the AS-IS carrier, simple techniques including analog filtering may be appropriate.

signals are nonlinearly absorbed above a preset threshold, and reflected below that threshold. Preliminary tests in the range of relevant frequencies (1-10 GHz) indicate that FISSS has suppression levels from 20-60 dB, and that digital communication signals may be reconstructed after FISSS processing to produce a bit-error rate (BER) of ~ 10^3 as compared to a BER = 0.5 (unusable noise) without FISSS.[9] The physical bulk of a connectorized version of FISSS is small (< 1 in^3) and the cost is anticipated to be low. FISSS, at least at first look, appears to permit certain tactical implementations of AS-IS to operate with an omnidirectional antenna[10] in a hostile electronic warfare (EW) environment.

---

9 This level of integrity of one incorrect bit per thousand correct bits is adequate for use with even simple error correction methods.

10 A directional antenna requires sensitive alignment, and is impractical as the primary receiver element for most AS-IS applications.

(This page is intentionally left blank)

IV. OTHER AS-IS IMPLEMENTATIONS

A. BASIC TACTICAL IMPLEMENTATIONS

While AS-IS has potential in exercising continuing authorization over nuclear and strategic weapons, the original development of the concept was aimed at the control of non-nuclear tactical weapons. Applications of AS-IS exist for any tactical system that relies on sophisticated electronics, including aircraft, tanks, missiles, etc. In this section, the implementation of AS-IS in tactical missiles, with specific examples given for man-portable surface-to-air missiles (SAMs) and anti-ship missiles, will serve to illustrate some of the general concepts involved. Unilateral implementation of AS-IS into tactical weapons intended for FMS and/or FMA is examined. Implications of these for various forms of "short-term diplomacy" are also discussed. Multinational implementation of AS-IS into tactical weapons, involving several or all of the major arms producing and supplying nations, would involve a significant degree of international cooperation, along with new treaties, but would have the strongest impact on the problems currently posed by uncontrolled proliferation.

1. Tactical Weapon Proliferation

The proliferation of high-threat tactical weapons, including anti-ship, ground-to-ground, and surface-to-air missiles, including man-portable Stinger-class SAMs, poses risks in both military and civilian arenas. The civilian sector is particularly threatened by terrorist groups and regimes, while the military sector is more broadly threatened. In the present context, a "high-threat" weapon is one that produces a high-kill and/or large casualty count per weapon dollar.[1] For this reason, these weapons often occupy a disproportionately large fraction of the arsenals of developing Third World countries and terrorist groups, relative to the makeup of arsenals of established regimes. As the guidance, targeting, and countermeasure-avoidance of tactical missiles become increasingly

---

1 In the case of transport aircraft and carriers, the respective counter-weapons represent less than 0.1% of the cost of the target. In rough terms, a $50,000 Stinger holds a $100 million aircraft at risk, while a handful of $1 million Exocets threaten a $5 billion aircraft carrier.

sophisticated, effective countermeasure systems are decreasing in availability. Those in use are often multi-tiered, and hence costly.

The inherent lack of continuing authorization over tactical weapons produced by a nation creates vulnerability to that nation due to unexpected loss or theft of weapons, or third party arms sales. Another situation arises when a formerly friendly regime becomes hostile and threatens to use weapons procured in prior arms sales against that nation, or its allies or interests. A recent example of the latter was the situation in the Persian Gulf, with Iraq using tactical weapons (e.g., SCUDs) previously supplied by the Soviets. Iraq also "inherited" numerous allied tactical assets, including Raytheon Patriot SAM-trackers, when it invaded Kuwait. The lack of benign continuing authorization over those weapons prevents them from being rendered harmless by the producing countries which, for the above cases, were the Soviet Union and United States.

Relative to strategic weapons, the safeguards afforded tactical weapons are minimal. The general PAL concept implemented in many nuclear weapons has not been applied to tactical weapons. Stingers are capable of being armed by a single individual from the day they enter the operational arena, and can only be disarmed with physical access. Minimal studies have been conducted relative to a system that directly parallels the nuclear-PAL. Systems that have been considered relied on physical access to grant authorization. The de facto dictum appears to emphasize countermeasures in contrast to retaining any degree of control over such tactical weapons.

The global situation has dramatically changed in the last 2 years or so. The apparent end of the Cold War, the attendant changing national alignments, and the Persian Gulf war all may drive bold new initiatives geared at regulating tactical weapons. A main driver for consideration of a continuing authorization system may be the desire to decrease the level of future conflicts that involve heavy use of externally procured weapons. It may not be wholly irresponsible to consider the possibility of new multilateral initiatives directed toward establishing some measure of continuing authorization over the use of tactical weapons. Given existing stockpiles, the benefit of an AS-IS system must be recognized as being predominantly long-term.

2. AS-IS Configuration for Tactical Weapons

A suitable example for discussion purposes is given by Stinger-type shoulder-fired SAMs. In such a weapon, the appropriate AS-IS default state would be 'DISABLE'. Reception of valid NCA transmissions would allow use of the weapon. In this case, the

effect of electronic jamming to drive the weapon into its default 'DISABLE' state is partly addressed by requiring infrequent message receipt (see also Section III.E). A clock internal to the AS-IS module within the missile launch tube enables the receiver and decoding electronics to detect and update the weapon's enable/disable status periodically (e.g., every 24 hours). This period could readily be contracted to minutes, or extended to weeks, months, or beyond. The weapon maintains status until the AS-IS module "wakes up" and listens for its next authorization transmission. To disarm a weapon, either a 'DISABLE' code may be broadcast for immediate effect, or the weapon address may be deleted from the NCA authorized-use list, in which case the weapon will be enter an appropriate disabled state after the current status period expires.

Operational considerations demand that field personnel need a capability to override the internal clock, using a launcher panel switch, to allow the weapon AS-IS status to be updated at any time. If this action is taken, the internal 24-hour clock is reset. Current status may be locked in by field personnel for a 24-hour period to ensure that jamming will have no effect during this period. This constant-status period cannot be extended without receiving a subsequent status update. Through such periodic updates, the service life of the battery is also extended approximately 500 times relative to the receiver being constantly enabled. For the power requirements in Section II.E, a relatively small 5 amp-hr lithium battery, housed in the launcher, provides nearly 10 months continuous service[2] and has a 5-year shelf life. The AS-IS hardware module has a compact and inexpensive omnidirectional antenna implemented with conformal microstrip technology in the launcher tube. Even for relatively small tactical weapons, such as Stinger-class SAMs, the 1 GHz carrier wavelength is well suited to an integral half-wave dipole antenna. Requisite signal processing electronics are also housed in the weapon or its launch platform, as shown in Figure 6.

To provide confidence to the soldier in the field, a status-lock switch is used to lock the current status for a prescribed period of time, which might be taken to be equal to the required message receipt interval, or 24-hours. This capability permits the soldier to predictably operate the weapon without concern that it may be disarmed at an inopportune time. This status-extension feature may be utilized only once after each valid authorization-code receipt. At any time the weapon operator may request a status update by enabling the

---

2 Higher capacity, or additional batteries, could be used to extend or eliminate the maintenance cycle.

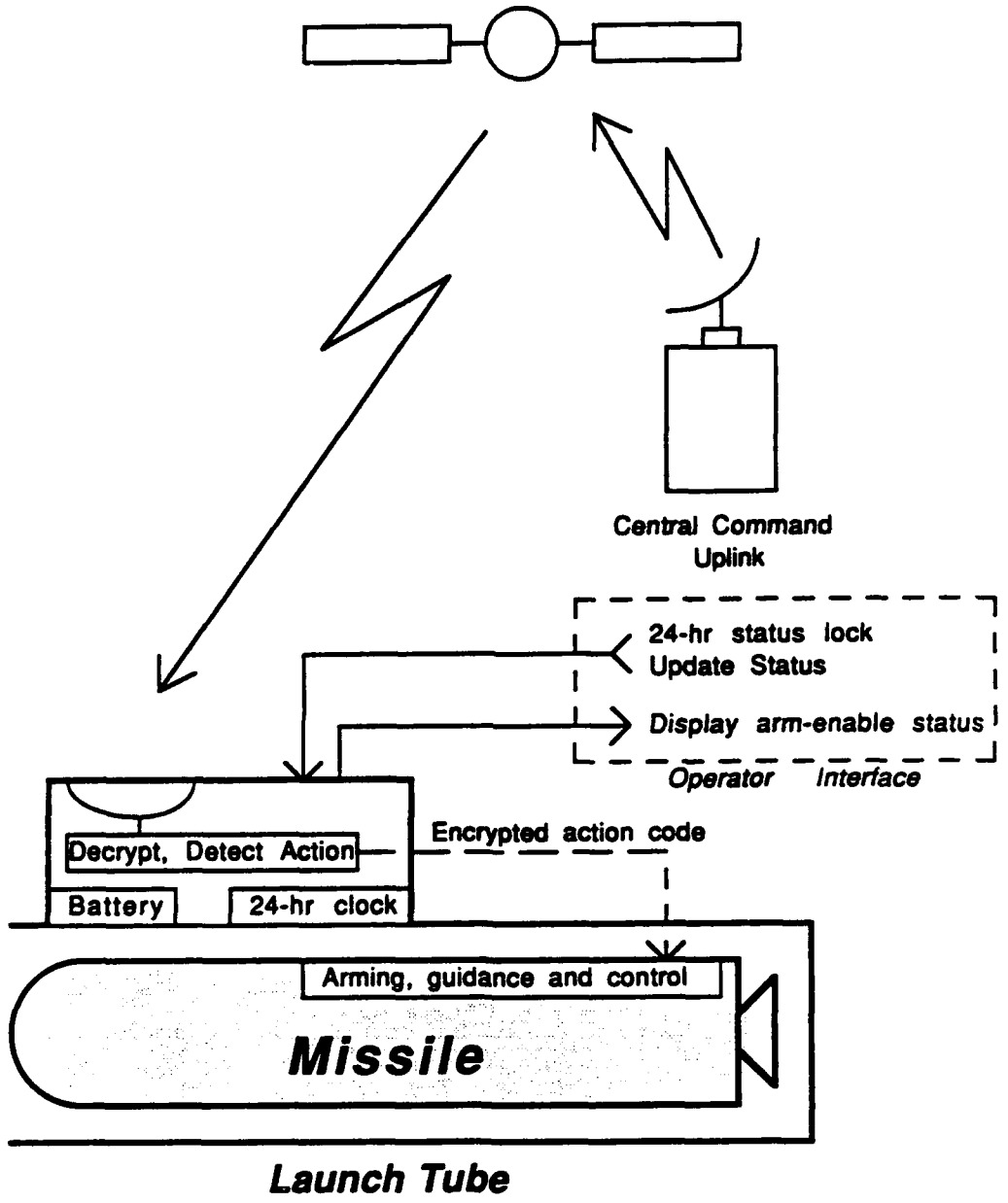


Figure 6. AI-IS Concept: Stinger Implementation

AS-IS module to actively listen for its particular code. This action might be taken when a weapon is uncrated and removed from an EM-shielded environment.

As shown in Figure 6, the only additional external features to the weapon system are the two switches noted above (to request status update and to lock current status) and one indicator lamp to display the current enabled/disabled status (e.g., green = 'ENABLED', red = 'DISABLED'). Other than the presence of the two switches and single indicator, no weapons operator actions are implied. Essentially, the AS-IS system is passive, and only requires minimal attention from the operator. Other elements such as an additional visual indicator or audible buzzer to indicate the impending termination of a 24-hour lockout period, as well as a feature that would permit automatic updating of current status during a lockout period, and extending the period if the status does not change, might also be considered.

3. Implications of AS-IS-Configured Tactical Weapons

AS-IS provides a means by which the threat level of certain tactical weapons is reduced, short of direct disarmament. To have a wider impact through multinational application of the concept to a sufficiently large percentage of weapons available globally, a number of diplomatic and political issues must be addressed. Some form of multinational treaty concerning the implementation of the AS-IS concept might even be considered. Such a treaty has multiple implications to arms manufacturers: not only must they accept the AS-IS concept, they also have to establish whether AS-IS provides a safer weapons environment that could drive proliferation[3] or whether it is restrictive, reducing the output of arms manufacturers in the signatory nations. Weapons using AS-IS are likely to vanish from terrorist arsenals and regimes. Does this imply that the arms market for tactical missiles and similar weapons simply shifts to Third World and other suppliers non-allied with AS-IS treaty nations? It might, but certainly the volume and quality of the weapons would decrease, with an increase in effective countermeasures against those weapons. Non-AS-IS weapons will probably use a lower level of technology, for which some countermeasures exist.

While certain issues related to the practical utility of multinational implementations of AS-IS in weapons for FMS remain unclear, an important and more straightforward application for AS-IS equipped tactical weapons arises in FMA situations (e.g., the

---

[3] A lower criterion may be established for sale of an AS-IS equipped unit versus a non-AS-IS unit.

Stingers widely believed to have been supplied to the Afghan mujaheddin). Given their functionality, AS-IS-equipped weapons could certainly be introduced more freely to help achieve a desired outcome in local or regional conflicts. AS-IS, in such situations, offers a potential for short-term diplomacy. The capability to introduce arms to an unstable arena for short term use, and subsequently render the arms harmless, is attractive in certain situations. AS-IS offers possibilities for convenient short-term weapon deployment to temporary allies (e.g., Iran or other Gulf nations in the August 1990 Iraq annexation of Kuwait) to fortify positions that would otherwise require U.S. or allied presence to control weaponry. An advantage is obtained in being able to rapidly increase fronts in a conflict theater, through a leveraging of indigenous human assets. Moreover, AS-IS equipped weapons provide an added degree of diplomatic and political pressure to be exerted on users, through the potential for temporarily disabling weapons, or else simply degrading their functionality (perhaps even covertly), to weigh the favor of battle in a desired direction.

B. GPS-COUPLED IMPLEMENTATIONS

Closely related to the basic tactical implementations listed above, when coupled with transmissions from GPS satellites, AS-IS provides for several entirely new and potentially interesting application scenarios. One of these involves the creation of weapons for FMS or FMA purposes having geographic specificity. In particular, a given weapon could be made to function within the confines of a preprogrammed set of GPS coordinates. Such weapons might thereby be functionally restricted to largely defensive purposes only. The precision with which the AS-IS-coupled passive GPS receiver can determine the weapons coordinates, even without selective availability, would allow the weapon to be restricted to work within, say, the borders of a particular country or a particular region.[4] The set of allowed geographic coordinates could even be reprogrammed by NCA via the AS-IS channel.

Another application involves coupling GPS and AS-IS for protection of sea power. For example, the AS-IS concept can applied to defend against anti-ship missiles. The key difference between the Stinger implementation and the anti-ship missile AS-IS unit is the addition of a GPS and second receiver. Although it is anticipated that many future weapons will have pre-existing GPS capability, the AS-IS GPS receiver is directly integrated into the tamperproof AS-IS unit. The GPS signal is used by the missile to

[4] With better than 100-meter accuracy.

establish a current position and direction vector (from the rate of change of position). To protect itself, a ship may routinely broadcast commands using a low-power signal transmitter (extending to roughly a 10-mile radius) to prevent incoming missiles from arming themselves. The disarm commands rapidly sequence through the relevant AS-IS unit addresses that correspond to the inbound weapons. In general, all weapons may be assumed to pose a threat. For example, if 10^6 missiles are to be prevented from maintaining arm-status within a 10-mile radius from the ship, a 2-GHz signal will ensure that an attacking missile would disarm itself within one-quarter second,[5] which is adequate for all known missiles.[6]

Instead of discretely addressing all possible AS-IS modules, a 'universal-disable' code could be implemented. This would require the broadcast of a single command that is recognized by all AS-IS equipped units. This lessens the bandwidth requirements of the system, but increases the burden of maintaining security of the universal code. The format of this direct ship-to-missile omnidirectional encrypted broadcast consists of a disarm (or arm-prevent) command, and the location of the ship. Upon receipt and decryption of this broadcast, the missile determines whether its range and directionality are such that the missile is within a prescribed range of the broadcast coordinates and if the velocity vector intersects those coordinates (i.e., the missile is heading toward the ship). This dual check permits missiles to be launched from a ship that is actively protecting itself against hostile fire, and to prevent the ship from inadvertently disabling other authorized missiles. Thus, AS-IS provides for the immediate incapacitation of a weapon only in a vicinity of a U.S. or friendly ship when that asset is threatened.

---

5 Worst-case scenario: the final code in a sequence of 10^6 512-bit codes (256 AS-IS bits, 256 encoded GPS bits) disarms the missile.

6 A Mach 2 missile at sea-level acquires the signal at 10 nautical miles and then travels less than 600 feet (one-tenth of a nautical mile) before disarming itself.

(This page is intentionally left blank)

V. SUMMARY AND FUTURE DIRECTIONS

The AS-IS concept described here is an RPAL, providing continuing authorization capability for advanced electronic systems. The concept is quite general, and implementations have been identified for strategic, tactical, and even commercial applications. AS-IS is structured around a set of globally transmitted secure action sequence messages-continuously sent by the NCA via one-way satellite links-to AS-IS receiver modules embedded in the weapons and coupled to their on-board arming/guidance circuitry. Individual AS-IS modules have unique digital addresses, allowing NCA to assert remote control or even remote programmability over entire classes of weapons, selected groups of weapons, or even over individual fielded weapons. No knowledge of the weapon or launch platform locations is required. The AS-IS units are receive-only and cannot disclose the presence of the weapon. If the NCA or the satellite link are compromised in any way, or if the AS-IS module itself is tampered with or fails for any reason, the weapon defaults to an appropriate predetermined functional state.

When configured for SLBM use, AS-IS appears to provide a potentially workable solution for the traditional objections against the use of PALs for naval nuclear strategic weapons. In particular, unlike conventional PALs, the AS-IS concept fully maintains the autonomous launch capability of the SSBN platform during wartime, which is central to the submarine's primary stabilizing role in the strategic triad, as well as the stealth characteristics of the submarine itself, while effectively allowing NCA to assert control over accidental or unauthorized SLBM launches during peacetime or in lower states of force readiness.

Appendix A gives a number of additional technical features of the AS-IS concept. Appendix B summarizes a Red Team Evaluation of the concept. The Red Team agreed that, on technical grounds alone, the AS-IS concept appears feasible, but the key issue on which further consideration of AS-IS hinges is the suitability of current Air Force PAL controls for naval nuclear missiles. If the present PAL system is considered insufficiently reliable for SLBM use, then the AS-IS concept may warrant further consideration.

Development of the AS-IS system is continuing. This is intended to lay the foundation for serious consideration of an AS-IS based remote continuing authorization system for advanced weapons.

REFERENCES

REFERENCES

[1] D.M. Nosenchuck, W.J.A. Dahm, & T.A. Prince, "AS-IS: Deterrence and Containment of High-Threat Tactical Weapons with Applications Ranging From Terrorist Threats to Carrier-Group Vulnerability." In *Summary Report of the FY 1989 and 1990 Activities of the Defense Science Study Group*, IDA Document D-942, pp. IV-4 – IV-25, April 1990, UNCLASSIFIED.

[2] D.M. Nosenchuck and W.J.A. Dahm, *Study and Demonstration of an Active Safing and Isolation System (AS-IS): A Remote Continuing Authorization Concept for Weapon Systems*. White Paper to the DARPA Advanced Systems Technology Office, Institute for Defense Analyses, Alexandria, VA, 26 September 1991, UNCLASSIFIED.

[3] J. Litva, J. Wang, and R. Fralich, *High-Performance Power Divider, Aperture-Coupled Patch Antenna, and Array Architecture Study*, Communication Research Laboratory, McMaster University, Report No. 210, October 1989.

[4] "Simple Circuit Instantly Cuts Jammer Signals," *Microwaves and RF*, pp. 135-140, September 1990.

(This page intentionally left blank)

APPENDIX A

THE AS-IS COMMUNICATIONS CONCEPT

Viewgraphs from a Presentation to a Red Team Convened at IDA

February 19, 1992

THE AS-IS COMMUNICATIONS CONCEPT

IDA

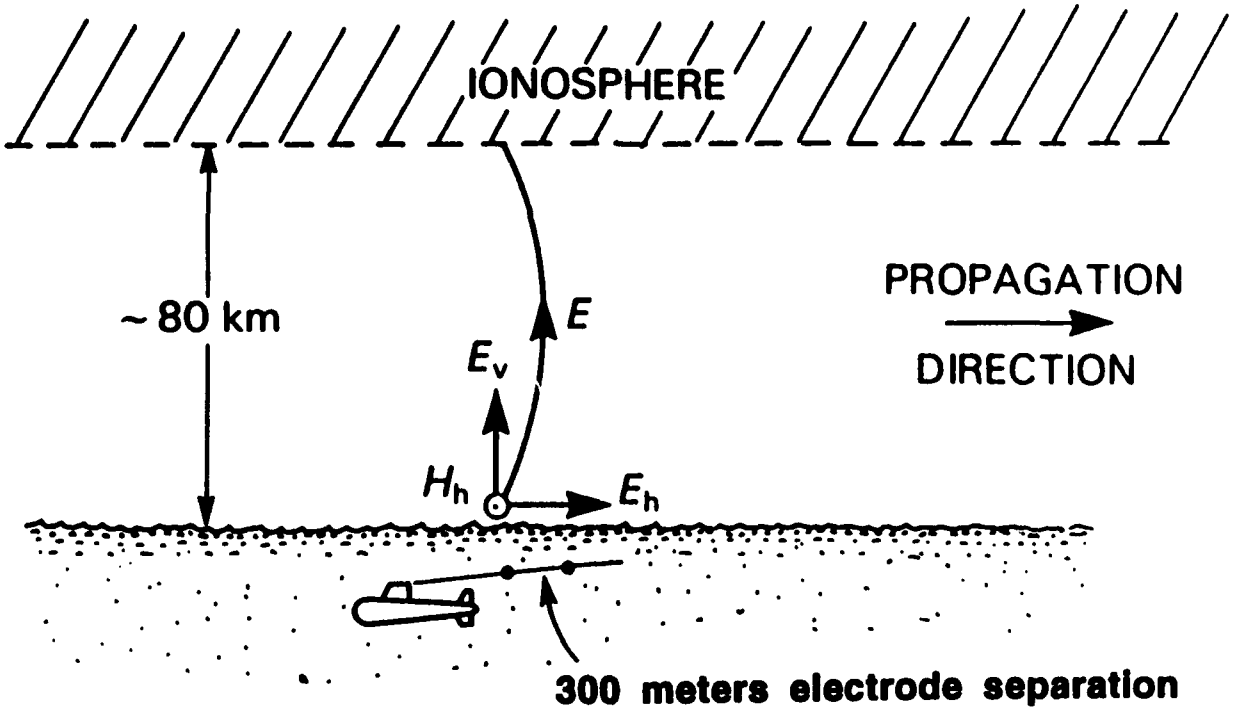
- AS-IS CONCEPT DISTINGUISHED BY
  - LOW-GRADE
  - DIRECT
  - OMNIDIRECTIONAL
  - ONE-WAY
  - SATELLITE-BASED
  - DIGITAL COMMUNICATIONS CHANNEL

- UNSUITABLE FOR TRADITIONAL COMMUNICATIONS APPLICATIONS

- POTENTIALLY SUITED FOR CERTAIN NARROW NICHE APPLICATIONS
  - STRATEGIC WEAPONS CONTROL
  - TACTICAL WEAPONS CONTROL
  - NOVEL COMMERCIAL APPLICATIONS

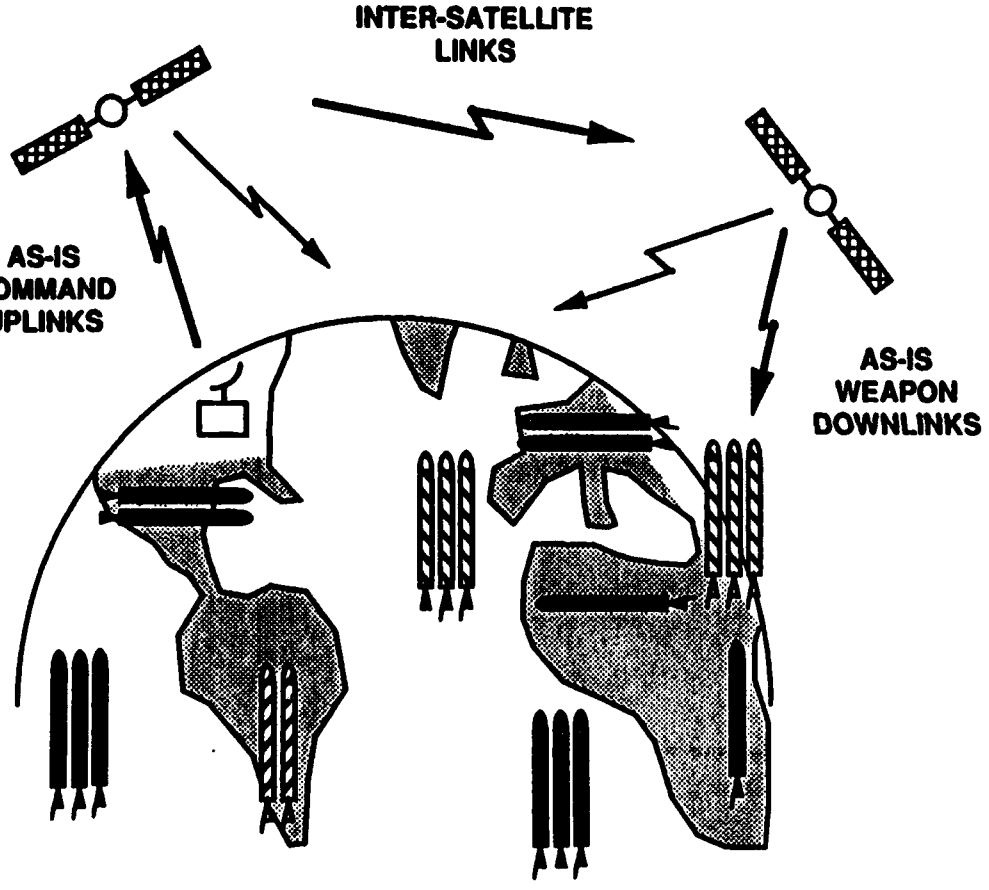
OTHER UNCONVENTIONAL NARROW NICHE LINKS

E.G., SUBMARINE COMMUNICATIONS OVER ELF (100 HZ) CARRIER

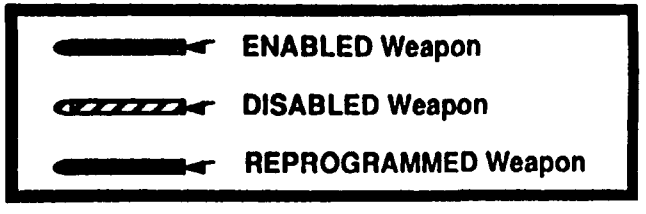


UNCLASSIFIED

THE GLOBAL AS-IS COMMUNICATIONS LINK



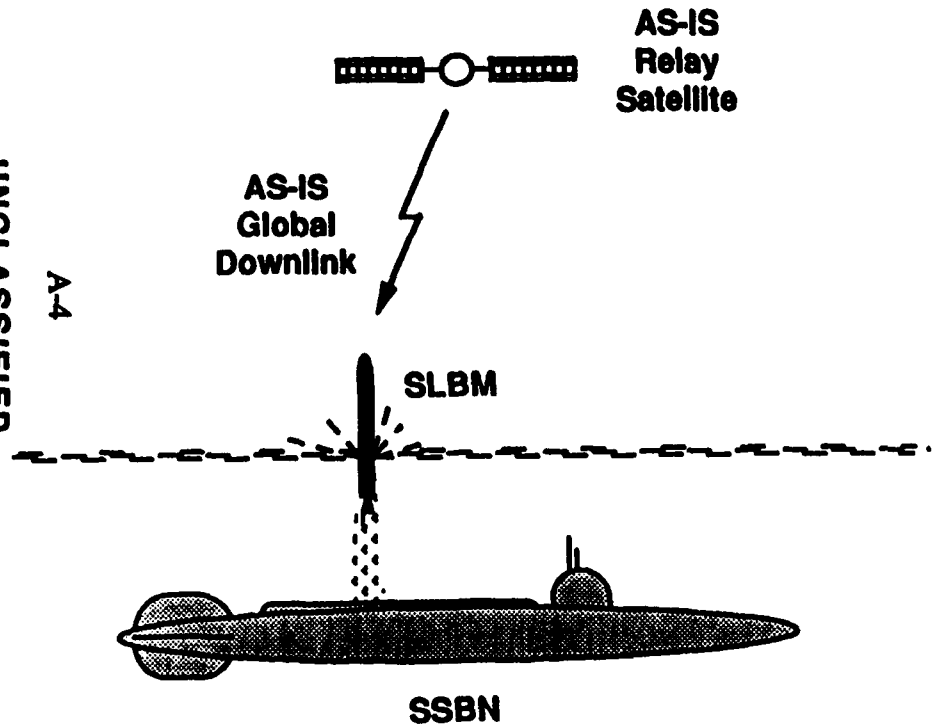
- NCA (MULTIPLE SITES)
- SATELLITE UPLINKS
- INTERSATELLITE LINKS
- WEAPON DOWNLINKS
- GLOBAL COVERAGE
- SECURE MESSAGES
- ONE-WAY TRANSMISSIONS
- EMBEDDED RECEIVERS
- OMNIDIRECTIONAL ANTENNA
- INDIVIDUAL WEAPON ADDRESSES



UNCLASSIFIED

UNCLASSIFIED

SLBM / SLCM COMMUNICATIONS LINK



- DEFAULT STATE IS 'ENABLE'
- AS-IS NEVER PREVENTS LAUNCH
- MESSAGE RECEPTION AT BREAKWATER
- NCA TRANSMITS 'DISABLE' CODE
- 0.1 SEC CYCLE TIME ACHIEVEABLE
- ALLOWS 'DISABLE' BEFORE MOTOR IGNITION
- DISARMS MISSILE / ABORTS FLIGHT
- MENU OF ACTION SEQUENCES AVAILABLE
- ROBUST UNDER ANY NCA LINK DISRUPTION
- POSITIVE LINK NEEDED ONLY TO BLOCK WEAPON USE

SLBM / SLCM APPLICATION DISTINGUISHED BY

- LOW LINK BANDWIDTH
- KNOWN MISSILE ORIENTATION AT BREAKWATER
- LARGE ANTENNA SIZE POSSIBLE

ALL OF THESE MAKE A HIGH-INTEGRITY LINK EASIER TO ESTABLISH

UNCLASSIFIED

A-4

UNCLASSIFIED

NCA UPLINK AND SATELLITE RELAY

IDA

- CONVENTIONAL UPLINKS AND RELAYS
- MULTIPLE NCA TRANSMISSION SITES
  - GROUND-BASED
  - AIRBORNE (E.G., LOOKING GLASS)
- REDUNDANT AND NETWORKED UPLINKS AND RELAYS
- ENCRYPTED MESSAGE TRANSMISSIONS
- SATELLITE RELAYS
  - GEO, LEO
  - EXISTING SATELLITES (NAVSTAR, MILSTAR, DSCS, FLTSAT)
  - INTER-SATELLITE LINKS

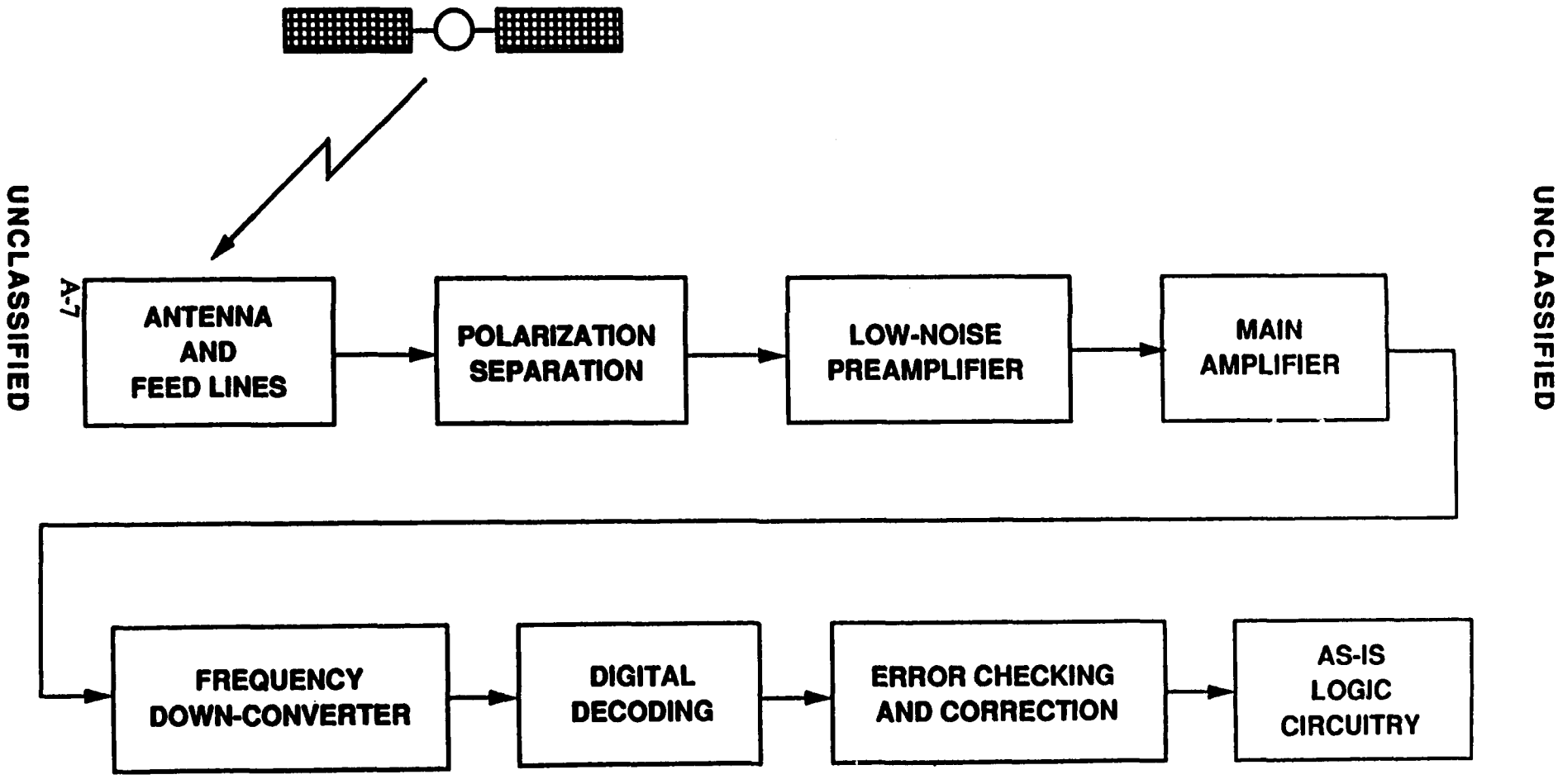
AS-IS DOWNLINK CHARACTERISTICS

IDA

- GLOBAL COVERAGE
- OMNIDIRECTIONAL
- CONFORMAL ANTENNA
- NO PHYSICAL ACCESS TO WEAPON REQUIRED
- NO KNOWLEDGE OF WEAPON LOCATION REQUIRED
- ADDRESSES INDIVIDUAL INSTALLED AS-IS RECEIVERS
- AS-IS RECEIVERS ARE STRICTLY PASSIVE
- NO WEAPON RESPONSE SIGNALS ARE TRANSMITTED
- RECEIVER LOGIC CONTROLS WEAPON FUNCTIONALITY

DOWNLINK INTEGRITY IS THE KEY TO PRACTICAL APPLICATION OF AN AS-IS COMMUNICATIONS LINK

AS-IS COMMUNICATIONS LINK COMPONENTS

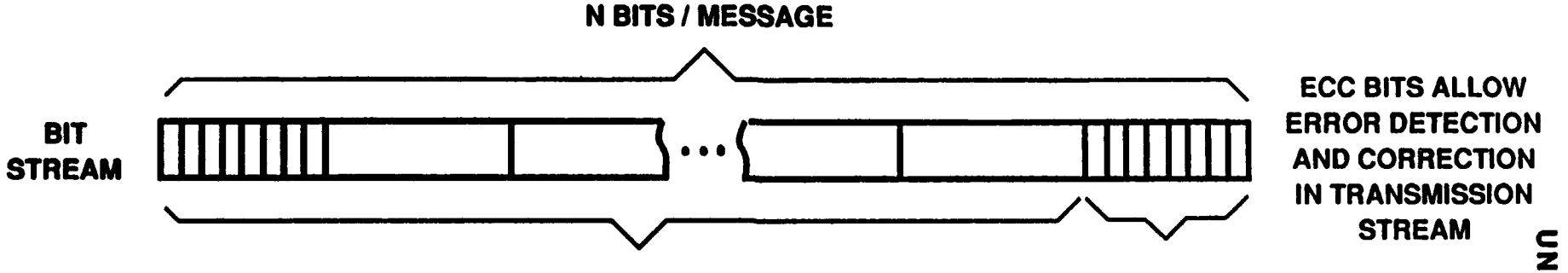


PRINCIPAL ERROR SOURCES IN COMMUNICATION LINK

- RECEIVER
  - THERMAL NOISE
  - FEED LINE LOSSES
- DOWNLINK
  - MULTIPATH INTERFERENCE
  - TROPOSPHERIC ABSORPTION
  - IONOSPHERIC POLARIZATION ROTATION
  - COSMIC NOISE
  - RAIN , FOG AND SNOW NOISE
- DIGITAL DECODING
  - QUANTIZATION ERROR
  - INTERSYMBOL INTERFERENCE
  - BIT SYNCHRO-OFF
  - CARRIER PHASE JITTER

UNCLASSIFIED

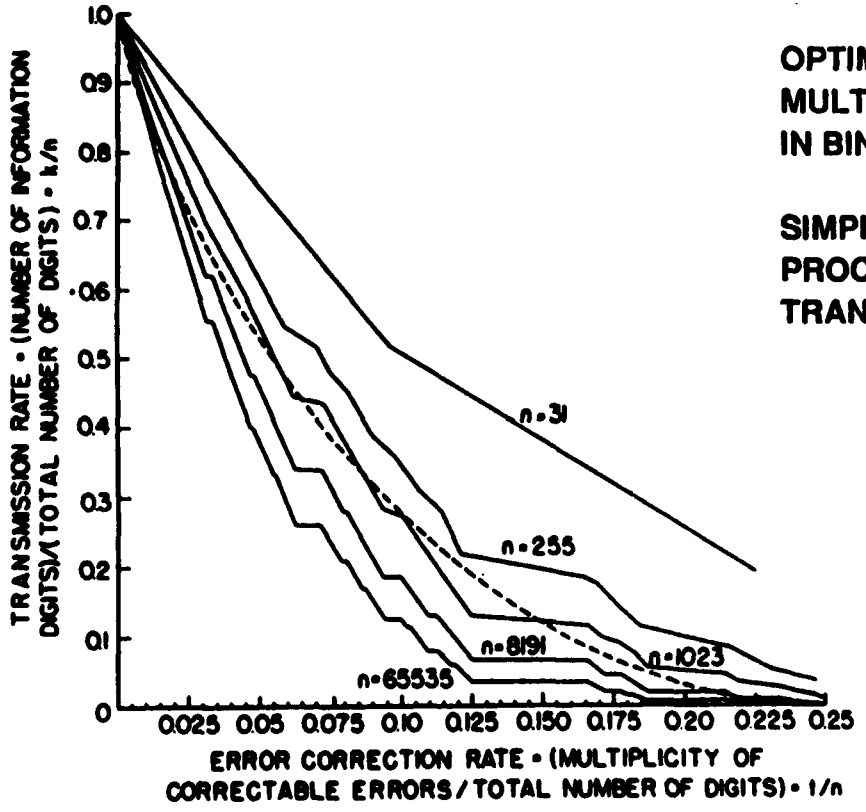
ERROR CHECKING AND CORRECTING (ECC)



- ADDRESS BITS
- DECRYPTION BITS
- ACTION SEQUENCE BITS

- (N, K) BINARY LINEAR BLOCK CODES
- CODE RATE EFFICIENCY : K / N
- ALL t - BIT ERROR PATTERNS CORRECTABLE
- MINIMUM HAMMING DISTANCE = $2t+1$
- AS-IS CODE FORMAT : N = 256, K = 192, BCH CODE

BINARY BOSE-CHAUDHURI-HOCQUENGHEM (BCH) CODES

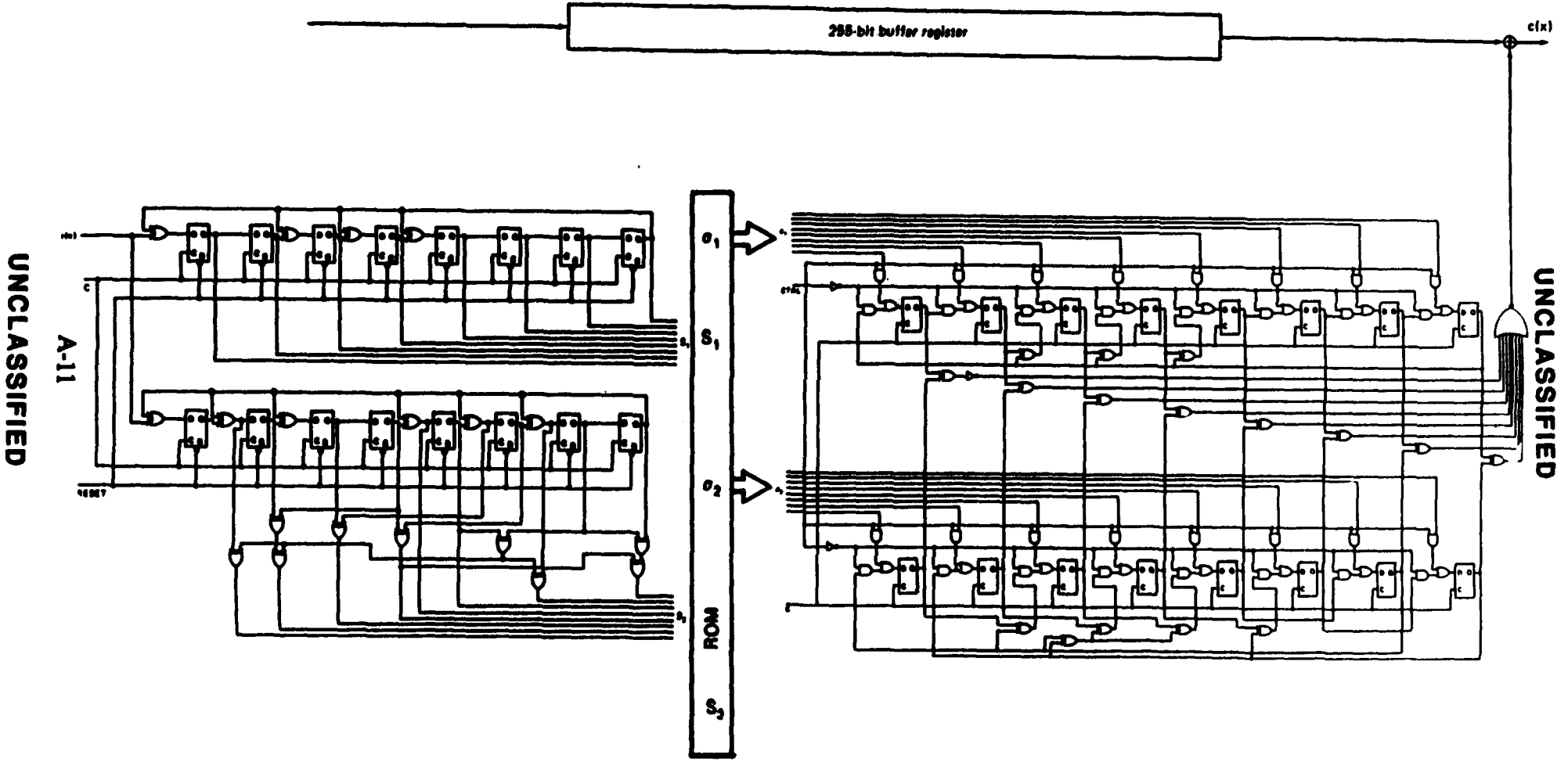


OPTIMAL HAMMING CODES FOR MULTIPLE RANDOM ERROR CORRECTION IN BINARY MESSAGES

SIMPLY IMPLEMENTED DECODING PROCEDURES EXIST FOR BINARY TRANSMISSIONS WITH BCH ECC

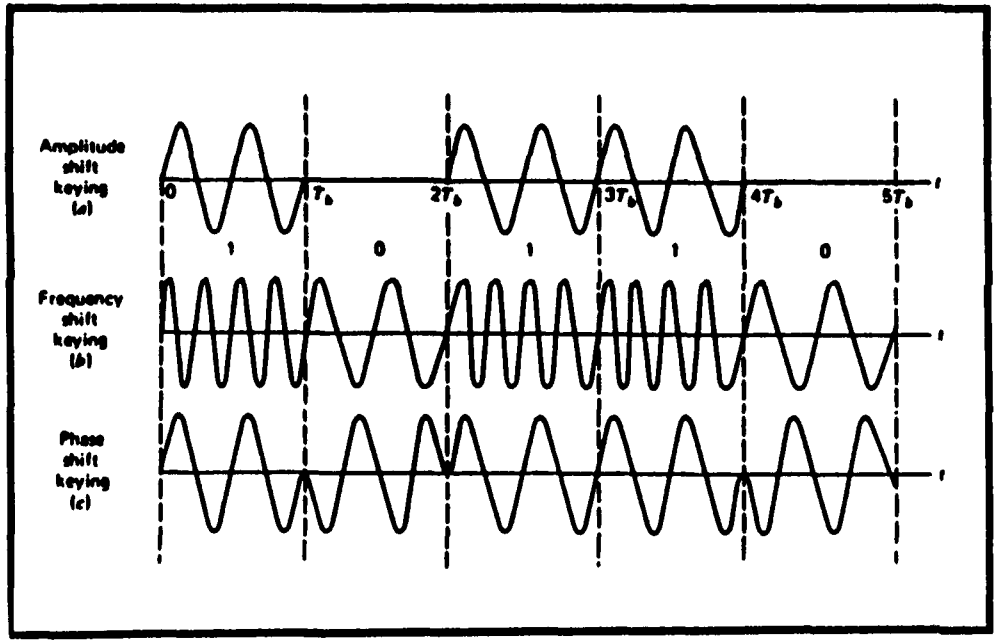
ALL ERRORS UP TO 9 BITS PER MESSAGE CAN BE CORRECTED FOR A (255,192) ECC BLOCK CODE WITH MINIMUM HAMMING DISTANCE OF 19

PRACTICAL IMPLEMENTATION OF BCH CODES



A (256,192) AS-IS BCH CODE IS SIMPLE TO IMPLEMENT USING TIME-DOMAIN TECHNIQUES

DIGITAL MODULATION SCHEMES



Scheme	P_e	S/N for $P_e = 10^{-4}$ (dB)	Equipment complexity	Comments
Coherent ASK	$Q\left(\sqrt{\frac{A^2T_b}{4\eta}}\right)$	14.45	Moderate	Rarely used $T\$ = A^2T_b/4$
Noncoh. ASK	$\frac{1}{2}\exp\left\{-\frac{A^2T_b}{16\eta}\right\}$	18.33	Minor	$T\$ = A/2$ $P_{e0} \neq P_{e1}$
Coherent FSK	$Q\left(\sqrt{\frac{0.61A^2T_b}{\eta}}\right)$	10.6	Major	Seldom used; performance does not justify complexity $T\$ = 0$
Noncoh. FSK	$\frac{1}{2}\exp\left\{-\frac{A^2T_b}{8\eta}\right\}$	15.33	Minor	Used for slow speed data transmission; poor utilization of power and bandwidth $T\$ = 0$.
Coherent PSK	$Q\left(\sqrt{\frac{A^2T_b}{\eta}}\right)$	8.45	Major	Used for high speed data transmission. $T\$ = 0$; best overall performance, but requires complex equipment
DPSK	$\frac{1}{2}\exp\left(-\frac{A^2T_b}{2\eta}\right)$	9.30	Moderate	Most commonly used in medium speed data transmission. $T\$ = 0$; errors tend to occur in pairs

UNCLASSIFIED

BIT ERROR RATES FOR DIGITAL CODING SCHEMES

IDA

- **BINARY FREQUENCY SHIFT KEYING (BFSK)**

$$P_e = \frac{1}{2} erfc\left(\frac{1}{2} S/N\right)^{1/2}$$

- **BINARY PHASE SHIFT KEYING (BPSK)**

$$P_e = \frac{1}{2} erfc(S/N)^{1/2}$$

- **QUAD PHASE SHIFT KEYING (QPSK)**

$$P_e = erfc\left(\frac{1}{2} S/N\right)^{1/2}$$

- **PULSE CODE MODULATION (PCM)**

$$P_e = \frac{1}{2} erfc \frac{1}{2}\left(\frac{1}{2} S/N\right)^{1/2}$$

- **DIFFERENTIAL COHERENT PHASE SHIFT KEYING (DCPSK)**

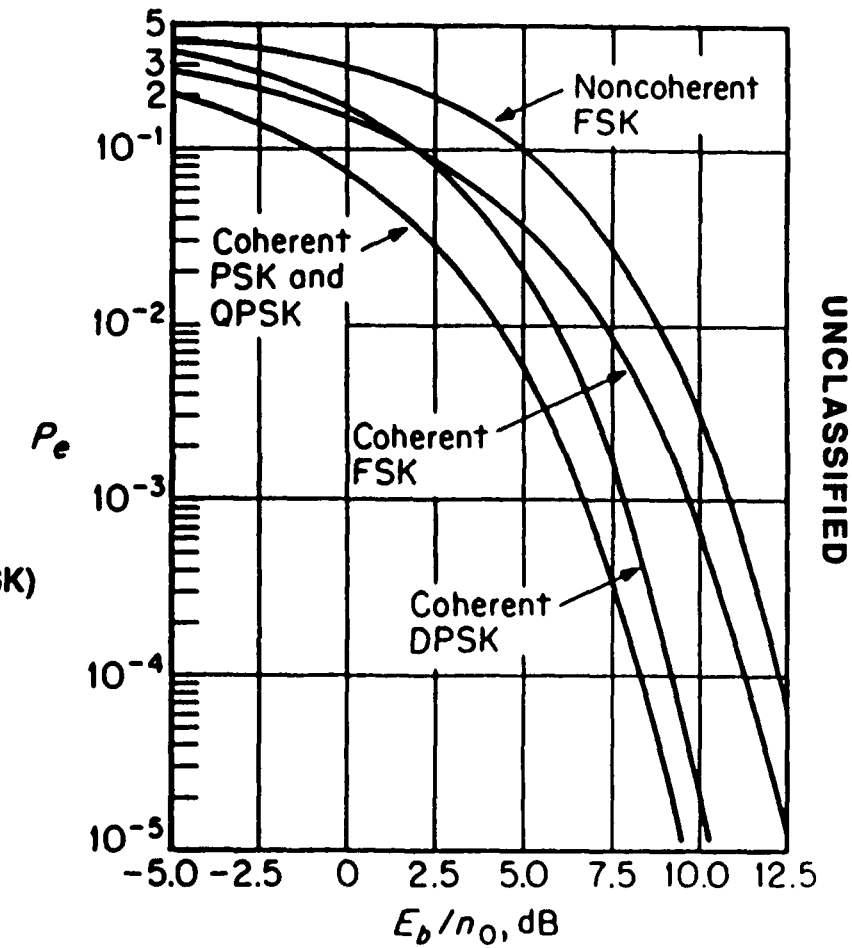
$$P_e = \frac{1}{2} exp\text{-}(S/N)$$

- **NON-COHERENT PHASE SHIFT KEYING (NCFSK)**

$$P_e = \frac{1}{2} exp\text{-}\frac{1}{2}(S/N)$$

- **NON-COHERENT AMPLITUDE SHIFT KEYING (NCASK)**

$$P_e = \frac{1}{2} exp\text{-}\frac{1}{4}(S/N)$$



UNCLASSIFIED

AS-IS COMMUNICATIONS LINK INTEGRITY ANALYSIS

- SINGLE 10-50 W SATELLITE DOWNLINK CHANNEL ASSUMED
- FULL HEMISPHERICAL PROJECTED COVERAGE
- ENERGY PER BIT ANALYSIS
- FREE-SPACE, ZERO-BACKGROUND THERMAL NOISE
- SIMPLE HALF-WAVE DIPOLE ANTENNA GAIN ASSUMED
- RESULTING BASELINE SNR DEPENDS ON:
  - CARRIER FREQUENCY
  - TRANSMISSION BANDWIDTH
  - DOWNLINK CHANNEL POWER

SIGNAL

$$E/BIT = \frac{P_T}{f_{BW}} \frac{A_R}{\frac{\pi}{4} D^2_{EARTH}}$$

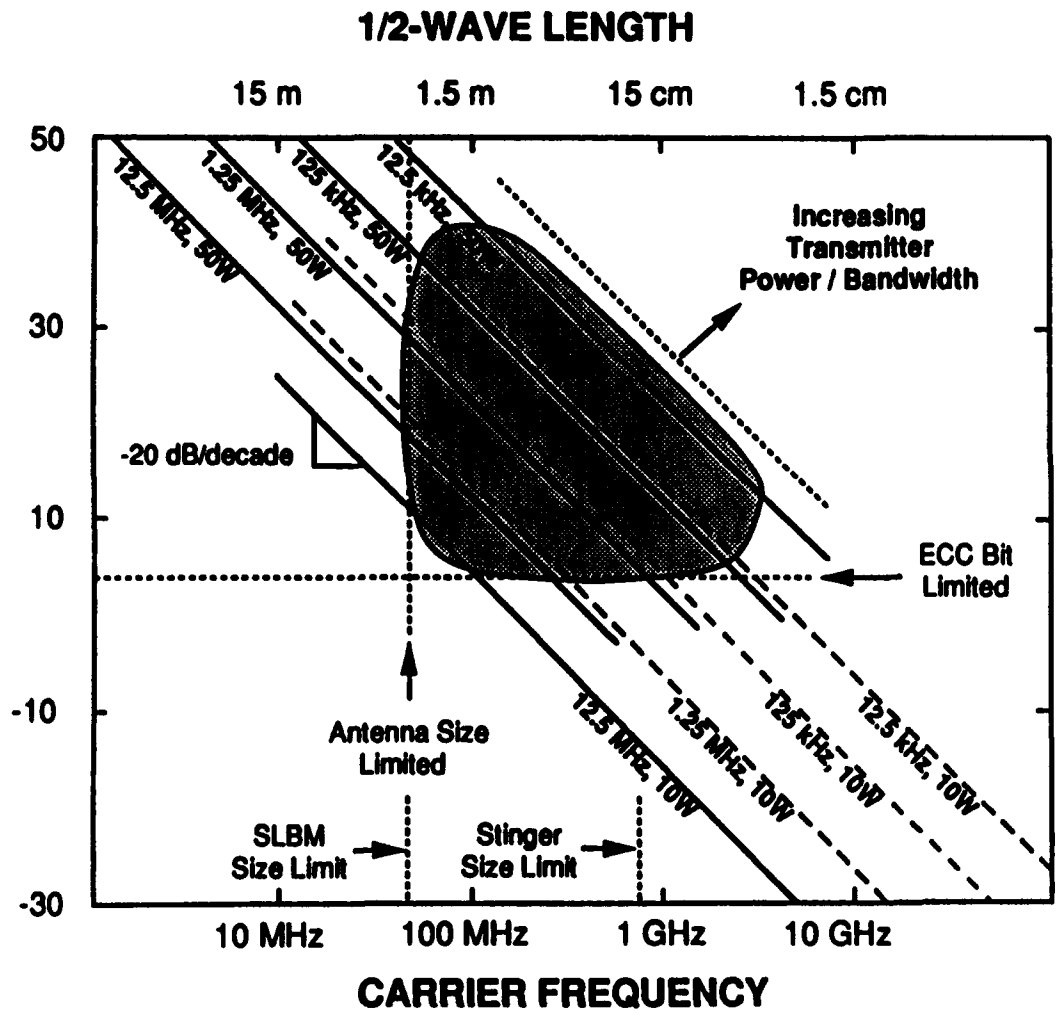
NOISE

$$E/BIT = kT$$

$$SNR = 225 + 10\ log\ P_T - 10\ log\ f_{BW} - 20\ log\ f_C$$

UNCLASSIFIED

AS-IS COMMUNICATIONS LINK INTEGRITY



LINK INTEGRITY INCREASED BY:

- DECREASED BANDWIDTH (10 dB/Decade)
- DECREASED CARRIER (20 dB/Decade)
- IINCREASED TRANSMITTER POWER

SUBJECT TO:

- ECC BIT LIMITATIONS
- ANTENNA SIZE LIMITATIONS
- TRANSMITTER POWER / BANDWIDTH

ACCEPTABLE SLBM LINK CONFIGURATIONS EXIST WITH BETTER THAN 50 dB INTEGRITY

UNCLASSIFIED

UNCLASSIFIED

AS-IS LINK DIRECTIONAL SENSITIVITY

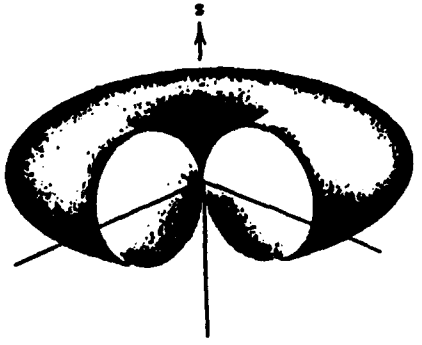
IDA

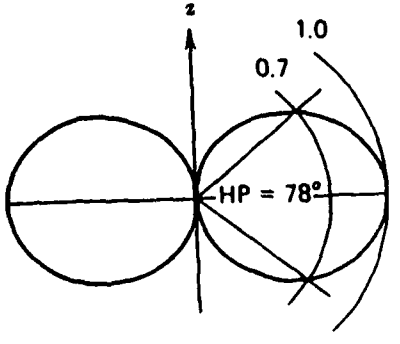
UNCLASSIFIED

HALF-WAVE DIPOLE ANTENNA DIRECTIVITY

$$D(\theta, \phi) = 1.64\left[\frac{\cos(\pi/2 \cos \theta)}{\sin \theta}\right]^2$$

$(L = \lambda/2)$.





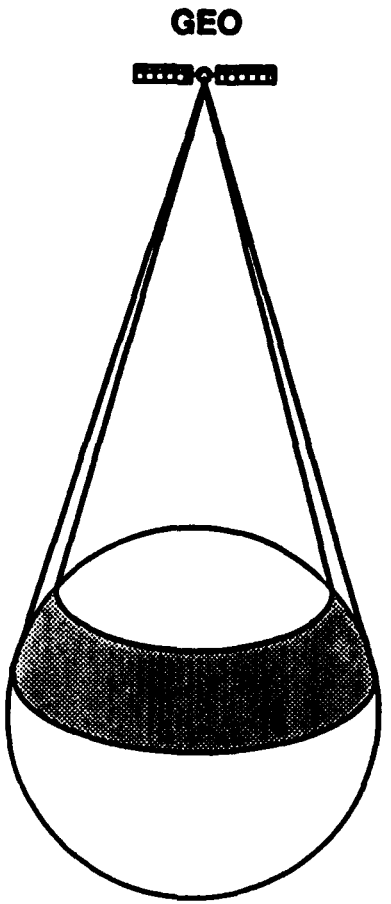
$L = \frac{\lambda}{2}$

- HALF-POWER (-3 DB) BEAMWIDTH IS 78 DEGREES

- -5 dB LIMIT ALLOWS RECEPTION 50 DEGREES ABOVE HORIZON

UNCLASSIFIED

–5 dB SINGLE SATELLITE COVERAGE

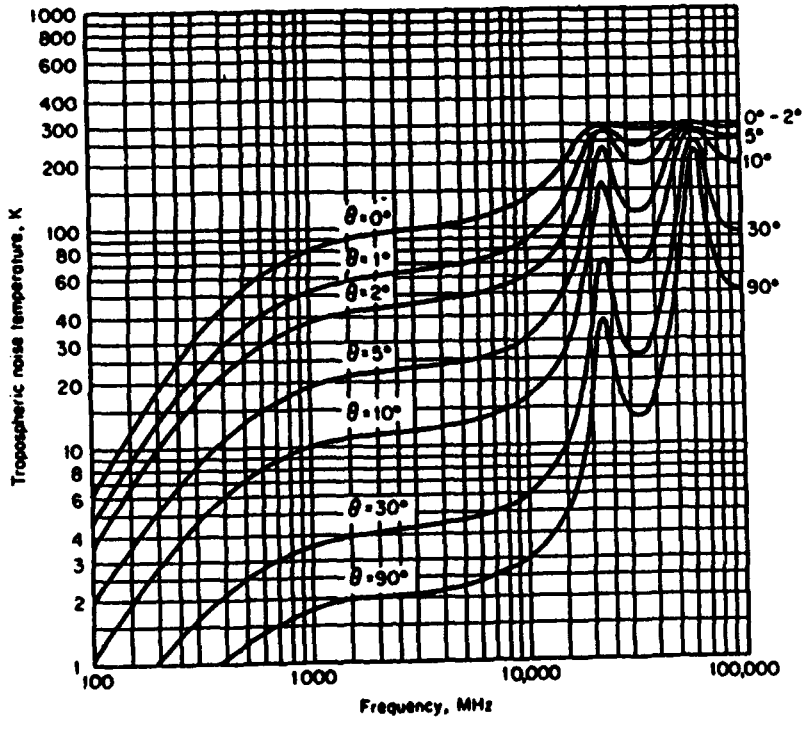


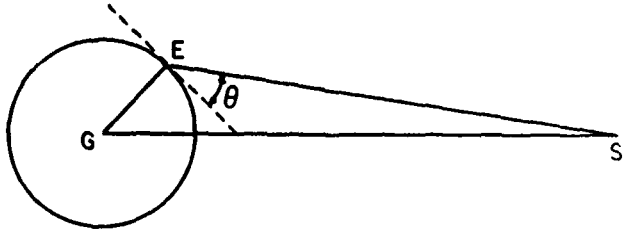
- SEVEN SATELLITE MINIMUM CONSTELLATION
  - FIVE OVERLAPPING ON EQUATORIAL ORBIT
  - TWO ON ±25-DEGREE INCLINED ORBITS FOR POLES
- EACH TRANSMITS IN TWO ORTHOGONAL POLARIZATIONS
- POLE-TO-POLE GLOBAL COVERAGE WITH OVERLAPS
- MORE SOPHISTICATED ANTENNA DESIGN ALLOWS LARGER AREA COVERAGE / FEWER SATELLITES

TROPOSPHERIC NOISE DEGRADATION

IDA

CONTRIBUTION TO EQUIVALENT SYSTEM NOISE TEMPERATURE VERSUS ELEVATION ANGLE AND FREQUENCY



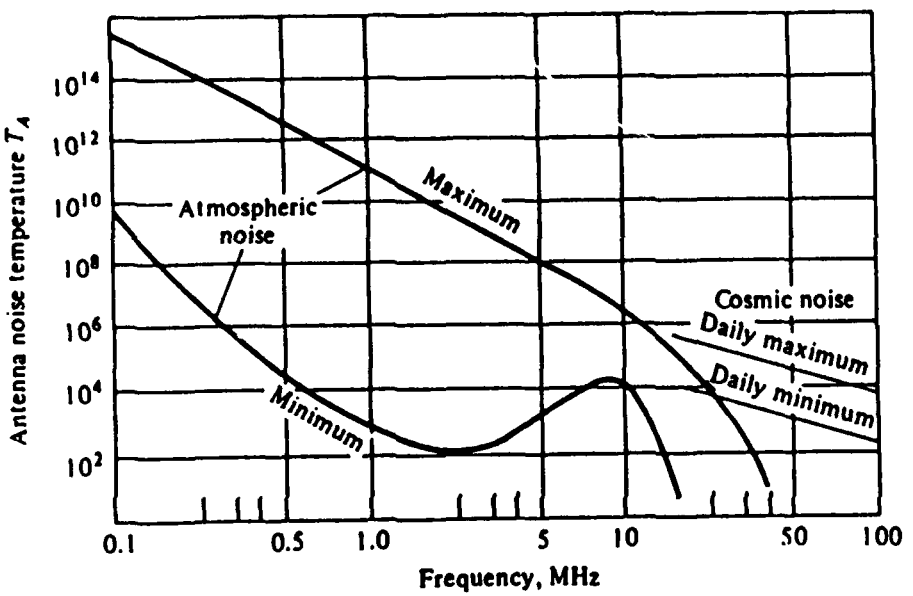


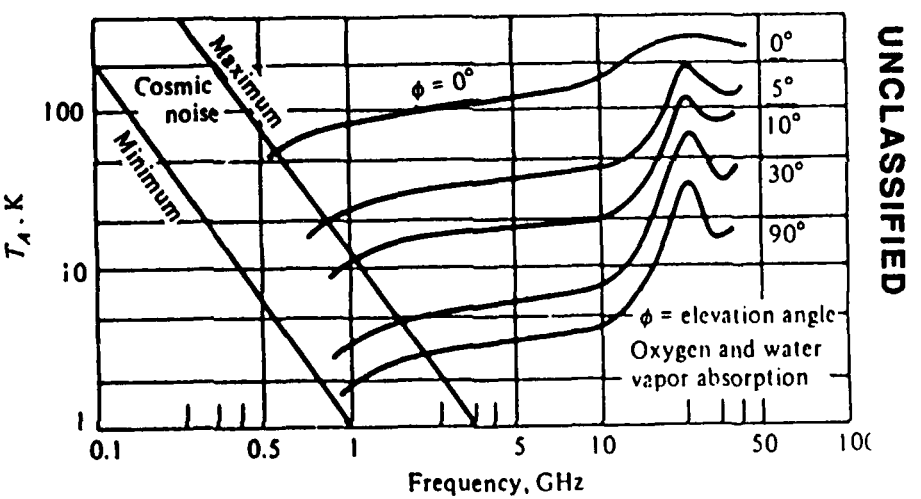
AT 1 GHz THIS LEADS TO LESS THAN 1 dB DEGRADATION

COSMIC AND ATMOSPHERIC NOISE DEGRADATION

IDA

CONTRIBUTION TO EQUIVALENT SYSTEM NOISE TEMPERATURE VERSUS FREQUENCY





FOR LOW CARRIER FREQUENCIES THIS CAN LEAD TO RELEVANT DEGRADATIONS

UNCLASSIFIED

RAIN NOISE DEGRADATION

IDA

CONTRIBUTION TO EQUIVALENT SYSTEM NOISE TEMPERATURE VERSUS FREQUENCY

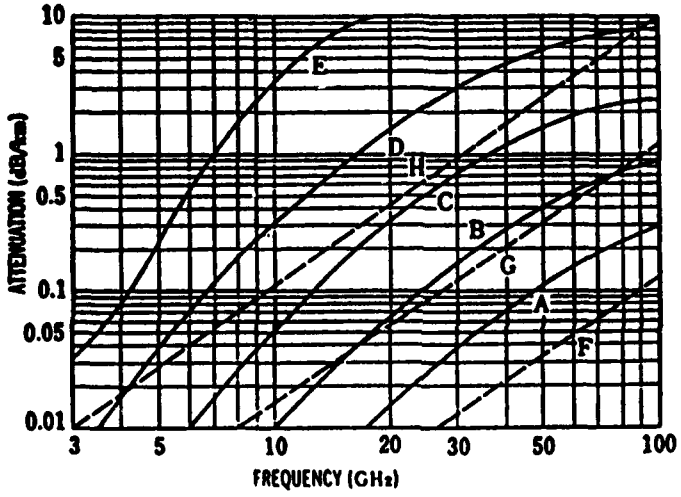


Fig. 1.7 Attenuation due to rainfall, fog or cloud (by CCIR)

——Attenuation in rainfall of intensity as

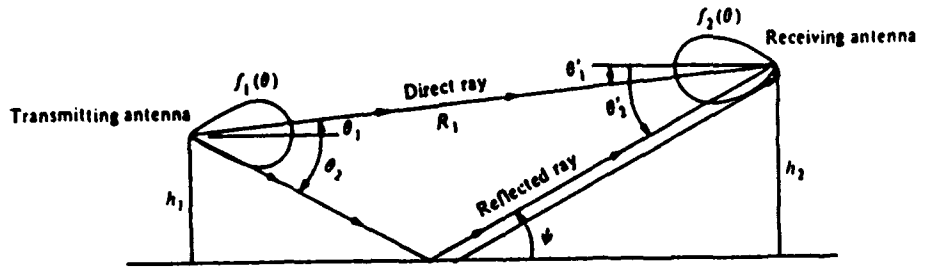
A: 0.25 mm/h (drizzle),
B: 1 mm/h (light rain)
C: 4 mm/h (moderate rain),
D: 16 mm/h (heavy rain),
E: 100 mm/h (very heavy rain).

– – –Attenuation in fog or cloud as

F: 0.032 g/m³ (visibility>600 m),
G: 0.32 g/m³ (visibility≈120 m),
H: 2.3 g/m³ (visibility≈30 m).

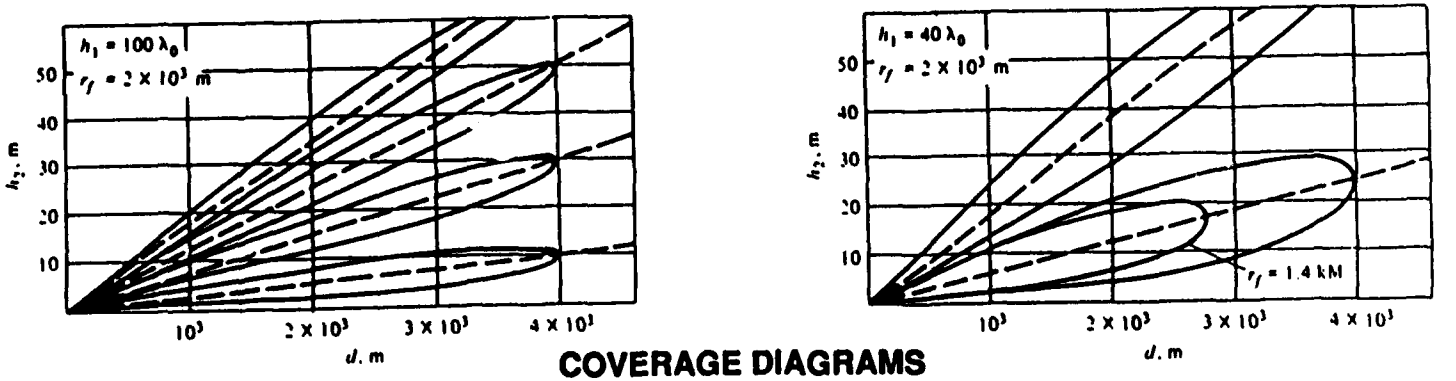
LESS THAN 1 dB DEGRADATION IN WORST CASE SENARIO

MULTIPATH INTERFERENCE EFFECTS



MULTIPATH REFLECTIONS

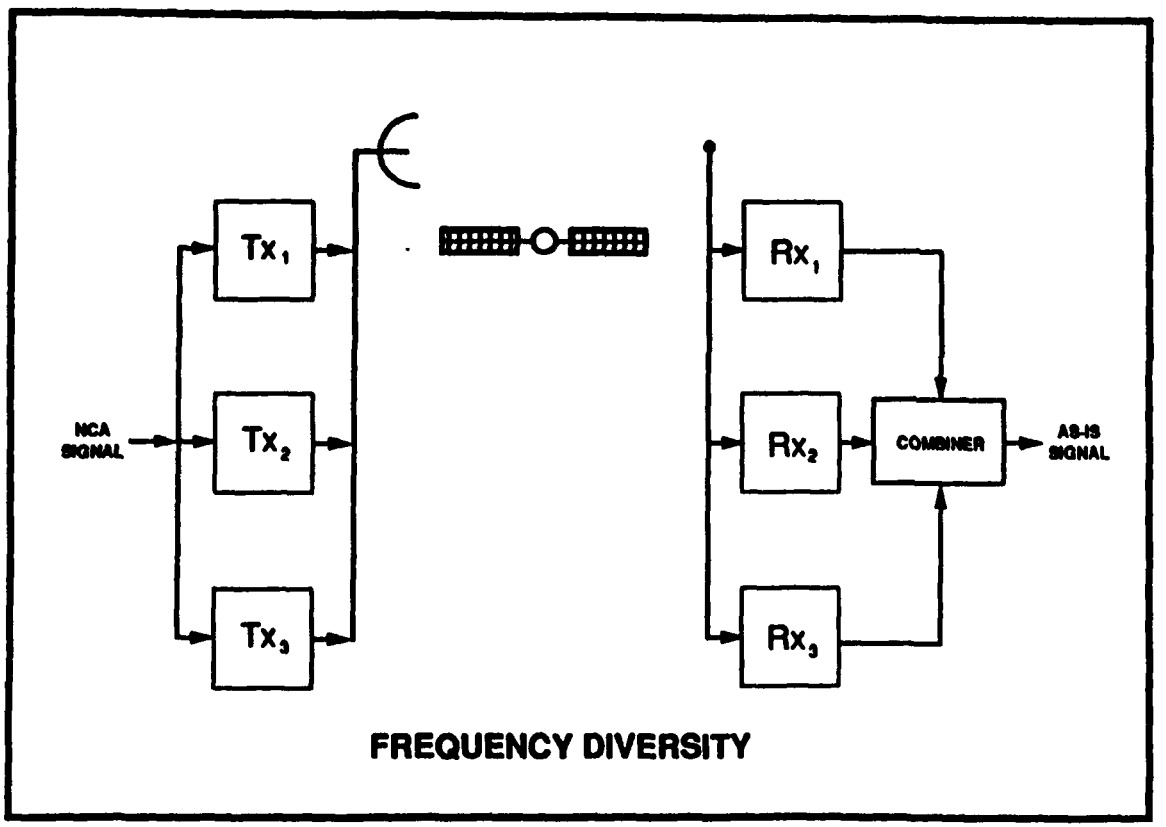
- DUE TO INTERFERENCE BETWEEN DIRECT PATH AND GROUND REFLECTIONS
- TYPICAL DELAY TIME (1 μSEC / MILE) ELIMINATES ECHO EFFECTS - REFLECTED SIGNAL ON SAME BIT
- RESULTING LOBE PATTERN IS HIGHLY FREQUENCY DEPENDENT, POLARIZATION DEPENDENT, AND DEPENDS ON NATURE OF SURFACE
- MULTIPATH INTERFERENCE CAN BE ESPECIALLY STRONG OVER CALM SEAS



COVERAGE DIAGRAMS

DESTRUCTIVE INTERFERENCE WITH REFLECTED PATH SIGNAL CAN SEVERELY DEGRADE LINK INTEGRITY FOR OMNIDIRECTIONAL ANTENNAS

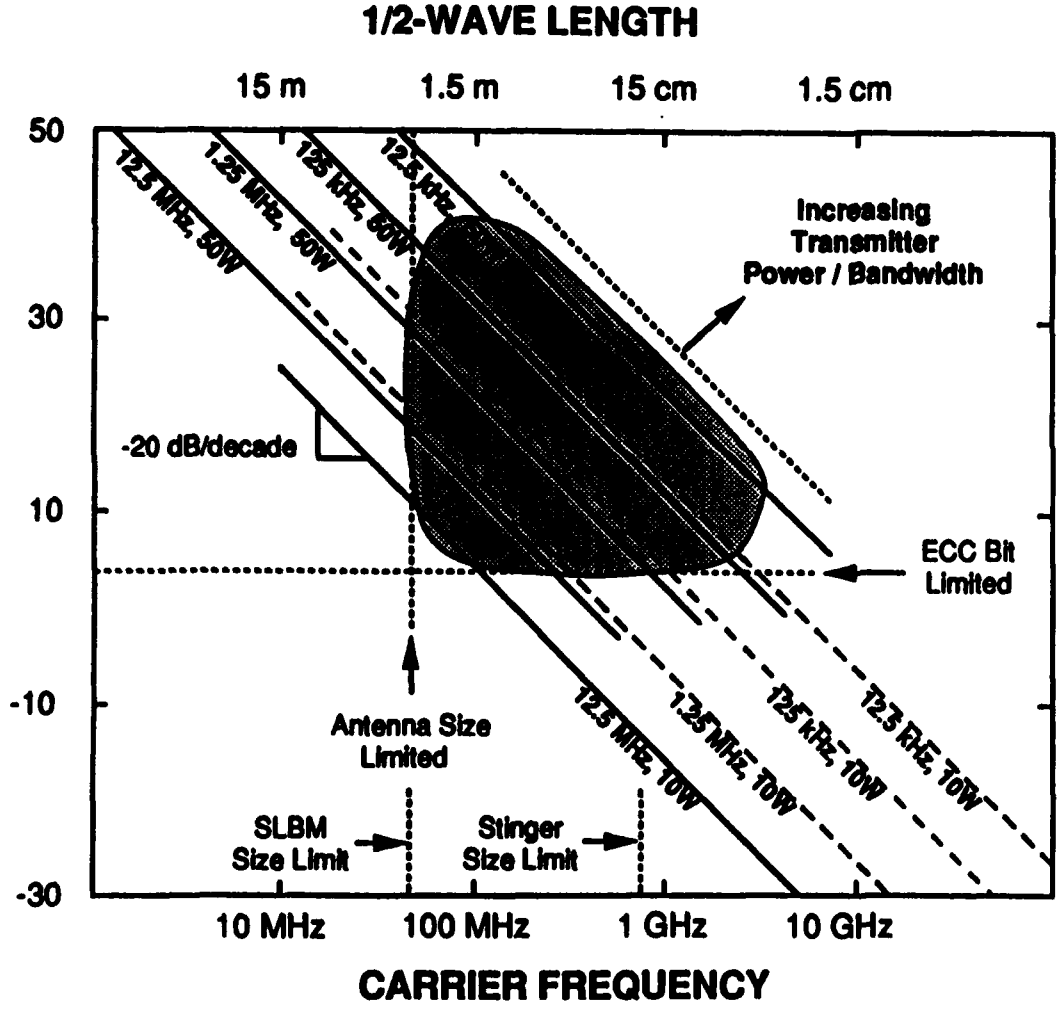
FREQUENCY DIVERSITY ELIMINATES MULTIPATH FADE



FREQUENCY DIVERSITY

- MULTIPLE FREQUENCIES ELIMINATE SIMULTANEOUS INTERFERENCE ON ALL CHANNELS
- FULL EQUIPMENT REDUNDANCY INCREASES OVERALL SYSTEM RELIABILITY
- FCC CURRENTLY PROHIBITS FREQUENCY DIVERSITY FOR COMMERCIAL USE TO AVOID SPECTRUM CROWDING
- LOW BANDWIDTH REQUIREMENTS FOR AS-IS ALLOW FREQUENCY DIVERSITY WITHOUT EXCESSIVE USE OF AVAILABLE SPECTRUM

OVERALL COMMUNICATIONS LINK INTEGRITY



- LINK INTEGRITY CAN BE MAINTAINED FOR SLBM APPLICATION AS WELL AS FOR WIDER TACTICAL LEVEL IMPLEMENTATIONS

UNCLASSIFIED

AS-IS COMMUNICATIONS LINK SUMMARY

- AS-IS COMMUNICATIONS LINK CONSISTS OF
  - LOW-GRADE
  - DIRECT
  - OMNIDIRECTIONAL
  - ONE-WAY
  - SATELLITE-BASED
  - DIGITAL COMMUNICATIONS CHANNEL
- LINK INTEGRITY CAN BE MAINTAINED AT BETTER THAN 10 dB
- ENSURES RELIABLE RECEPTION AND DECODING OF AS-IS SIGNALS
- CAN BE FULLY IMPLEMENTED WITH EXISTING TECHNOLOGY
- POTENTIALLY SUITED FOR CERTAIN NARROW NICHE APPLICATIONS
  - STRATEGIC WEAPONS CONTROL
  - TACTICAL WEAPONS CONTROL
  - NOVEL COMMERCIAL APPLICATIONS

UNCLASSIFIED

AS-IS DEFAULT FUNCTIONALITY

IDA

- WEAPON DEFAULTS TO PREDETERMINED FUNCTIONAL STATE AUTOMATICALLY IF VALID NCA AS-IS MESSAGE IS NOT RECEIVED BEFORE PRESCRIBED UPDATE PERIOD EXPIRES
- DEFAULT OCCURS WHENEVER NCA TRANSMISSIONS ARE :
  - BLOCKED
  - INTERRUPTED
  - COMPROMISED
  - TERMINATED
- SLBMs / SLCMs REMAIN IN THEIR DEFAULT STATE UNTIL BREAKWATER
- DEFAULT STATE FOR SLBMs / SLCMs IS 'ENABLED'
- 'ENABLED' STATE PROVIDES FULL WEAPON FUNCTIONALITY, AS IF AS-IS WERE NOT PRESENT
- AS-IS NEVER PREVENTS MISSILE LAUNCH, ONLY DEALS WITH CONTROL AFTER AN UNAUTHORIZED / ACCIDENTAL LAUNCH
- DEFAULT CAPABILITY DOES NOT INTERFERE WITH PEACETIME OR WARTIME OPERATIONS
- DEFAULT FUNCTIONALITY ALLOWS SLBMs / SLCMs TO :
  - MAINTAIN CURRENT LAUNCH AUTONOMY
  - MAINTAIN CURRENT STEALTH OPERATIONS
  - MAINTAIN ULTIMATE STABILIZING ROLE IN STRATEGIC TRIAD

AS-IS IS THE OPPOSITE OF A CONVENTIONAL PAL

IDA

CONVENTIONAL PALs	AS-IS
• GENERALLY REQUIRE PHYSICAL ACCESS TO THE WEAPON	• REQUIRES NO PHYSICAL ACCESS TO WEAPON, NOR EVEN KNOWLEDGE OF WEAPON LOCATION
• REQUIRE A POSITIVE ACTION SEQUENCE TO PERMIT WEAPON FUNCTIONALITY	• POSITIVE ACTION SEQUENCE IS REQUIRED ONLY TO BLOCK WEAPON FUNCTIONALITY
• GENERALY INVOLVE WEAK LINK THROUGH EXTERNAL LAUNCH AUTHORIZATION MESSAGE	• NO EXTERNAL LAUNCH AUTHORIZATION MESSAGE IS REQUIRED, FULL LAUNCH AUTONOMY MAINTAINED
• GENERALLY INTERFERE WITH SSBN STEALTH CHARACTERISTICS AND LAUNCH AUTONOMY	• NO EFFECT ON SSBN STEALTH CHARACTERISTICS OR ON LAUNCH AUTONOMY
• REDUCE SLBM / SLCM STABILIZING ROLE IN STRATEGIC TRIAD	• FULLY MAINTAINS SLBM / SLCM STABILIZING ROLE IN STRATEGIC TRIAD

UNCLASSIFIED

A-26

UNCLASSIFIED

AS-IS EFFECTIVELY INTRODUCES :

1. A CAPABILITY FOR NCA TO ASSERT CONTROL OVER ACCIDENTAL / UNAUTHORIZED MISSILE LAUNCHES IN PEACETIME OR LOWER STATES OF FORCE READINESS
2. WITHOUT COMPROMISING SSBN OPERATIONS IN PEACETIME OR WARTIME

TACTICAL VS. STRATEGIC AS-IS IMPLEMENTATIONS

STRATEGIC

- DEFAULT STATE IS 'ENABLED'. AS-IS PROHIBITS USE OF THE WEAPON.
- RELATIVELY SMALL NUMBER OF INDIVIDUAL WEAPONS TO BE CONTROLLED.
- MESSAGE TRANSMISSION OCCURS OVER SHORT UPDATE PERIOD.
- MODULE AUTOMATICALLY LISTENS FOR ITS ADDRESS AND NEW STATUS.
- NO USER OPERATIONS IMPLIED BY PRESENCE OF AS-IS MODULE.

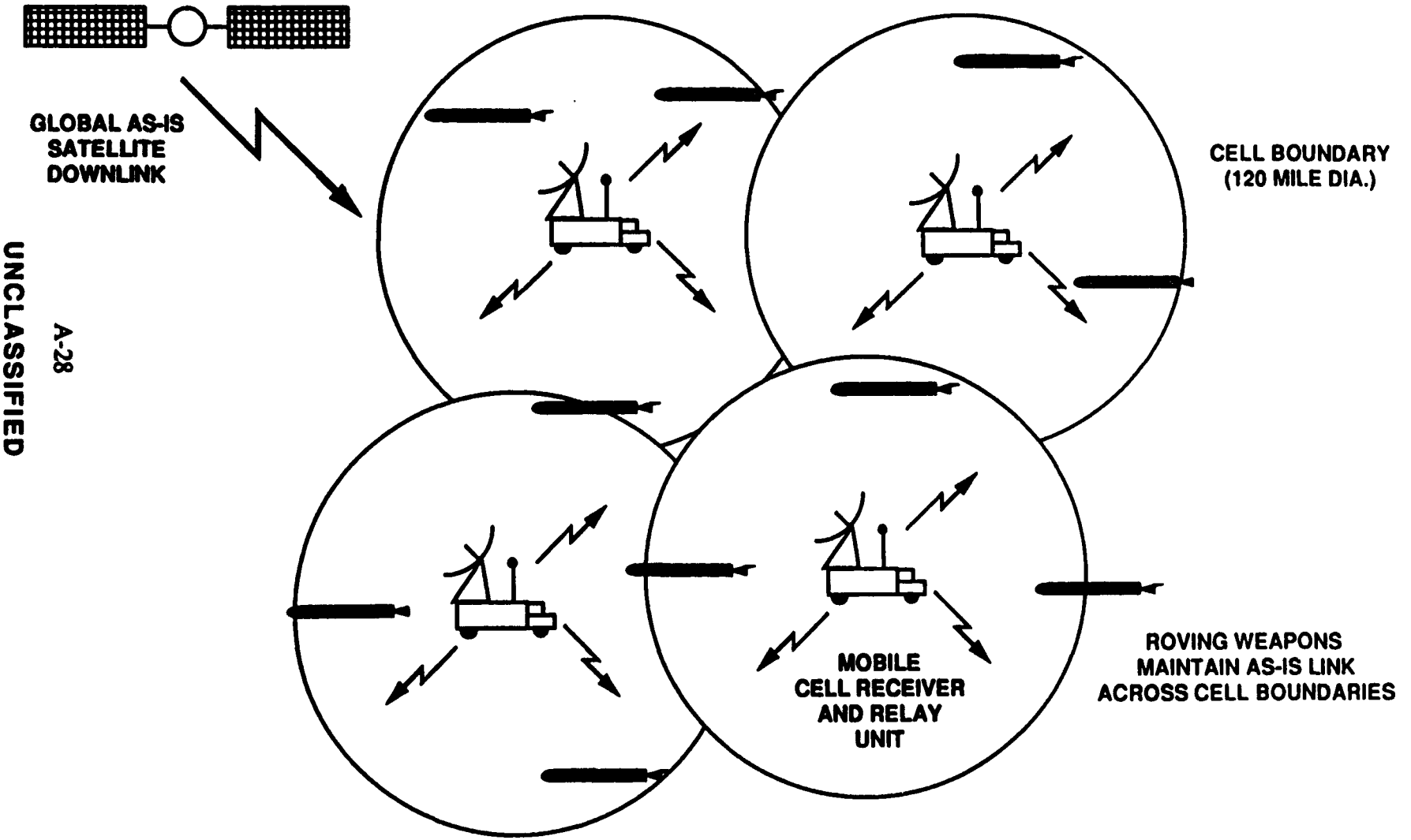
TACTICAL

- DEFAULT STATE IS 'DISABLED'. AS-IS PERMITS USE OF THE WEAPON.
- NUMBER OF INDIVIDUAL WEAPONS TO BE CONTROLLED IS LARGE.
- CURRENT STATE LOCK FEATURE REQUIRES INFREQUENT AS-IS STATUS UPDATE.
- IMMEDIATE STATUS UPDATE FEATURE PERMITS MESSAGE-LISTEN MODE ON DEMAND.
- CHECK-STATUS DISPLAY, UPDATE PERIOD EXPIRATION, ETC.

POTENTIAL TACTICAL APPLICATIONS IN :

- FOREIGN MILITARY AID (FMA) WEAPONS
- FOREIGN MILITARY SALES (FMS) WEAPONS

CELLULAR MODE FOR TACTICAL WEAPON CONTROL



AS-IS MESSAGE SECURITY

IDA
DEFENSE SCIENCE STUDY GROUP

- All transmissions from the NCA are encrypted
- Encoded time-stamps counter pre-recording and playback
- Message length is short: 256-bits
- Messages are broadcast in random sequences
- Public Key / Private Key is proposed as basic cryptosystem
  - Encryption keys are publicly known
  - Decryption keys unique to AS-IS receiver
  - Decryption key comprised of hard and soft fragments
  - Authentication of sender (NCA or any other source) identity
  - Authorized 'users' may be added or deleted without compromise

AS-IS MESSAGE FORMAT

IDA
DEFENSE SCIENCE STUDY GROUP

256-bit AS-IS message:

Header	Unit Address	Command	New Key Frag	Authenticator/Time	Random Cyphertext	ECC/Parity
14 bits	*24 bits*	*16 bits*	*48 bits*	*40 + 40 bits*	*24 bits*	*50 bits*

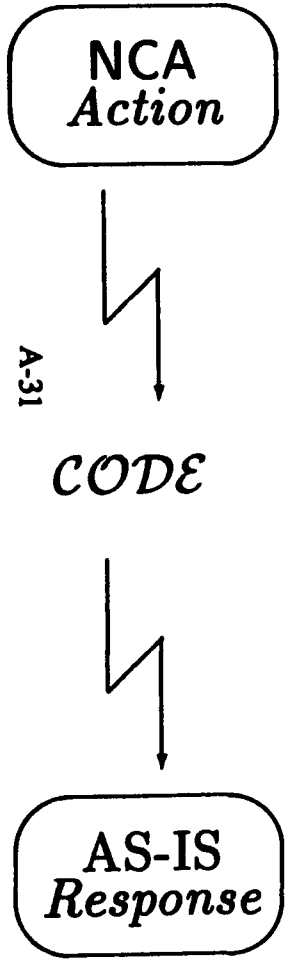
UNCLASSIFIED

- FIELDS:
  - Header: Indicates start of message
  - Unit Address: 16 million unique units
  - Command: Arm, disarm, reprogram function and/or target coordinates, etc
  - New Key Fragment: Soft portion of two-part prime number key
  - Authenticator/Time: NCA 'signature' and message time-stamp (35,000 yr, 1-sec precision)
  - Random Cyphertext: Digital 'noise' and/or additional (required) cypher bits
  - ECC/Parity: 7 error-correcting and 1 parity bit per 32-bit block, excluding header

UNCLASSIFIED

EXAMPLE: RSA CRYPTOSYSTEM

IDA
DEFENSE SCIENCE STUDY GROUP



- Implement $\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$ where
  - plaintext and cyphertext message-units are k and l 'letters' in respective length, with $k < l$
  - N-letter 'alphabet'
  - each unit has two secure prime numbers, p and q
  - public encryption key $K_E = (n, e)$ used to generate f
  - private decryption key $K_D = (n, d)$ used to generate f^{-1}
  - NCA sends $\mathcal{C} = f(\mathcal{P})$
  - AS-IS module performs $f^{-1}(\mathcal{C}) = f^{-1}f(\mathcal{P}) = \mathcal{P}$
- RSA functions:

  $f = \mathcal{P}^e \bmod n$:

  where $N^k < n = pq < N^l$; e 'random'

  $f^{-1} = \mathcal{C}^d \bmod n$

  where $d = e^{-1} \bmod (p-1)(q-1)$

UNCLASSIFIED

UNCLASSIFIED

NCA SIGNATURE AUTHENTICATION

IDA
DEFENSE SCIENCE STUDY GROUP

- User A (eg., NCA) wants to send a signature $\mathcal{S}$ as code $\mathcal{C}$ to User B (AS-IS receiver)
- $\mathcal{S}$ is a signature (eg., random prime number, code phrase, time-stamp)
-

User	Public Key	Private Key
A:	(n_a, e_a)	(n_a, d_a)
B:	(n_b, e_b)	(n_b, d_b)

- User A knows own private key and B's public key
- If $n_a < n_b$, User A sends $\mathcal{C} = f_B f_A^{-1}(\mathcal{S})$, or

$$\mathcal{C} = \left(\mathcal{S}^{d_A} \bmod n_A\right)^{e_B} \bmod n_B$$

- User B, knowing A's public key, performs the inverse operation

$$\begin{aligned} f_A f_B^{-1}(\mathcal{C}) &= f_A(f_B^{-1} f_B) f_A^{-1}(\mathcal{S}) \\ &= f_A \cdot 1 \cdot f_A^{-1}(\mathcal{S}) \\ &= \mathcal{S} \end{aligned}$$

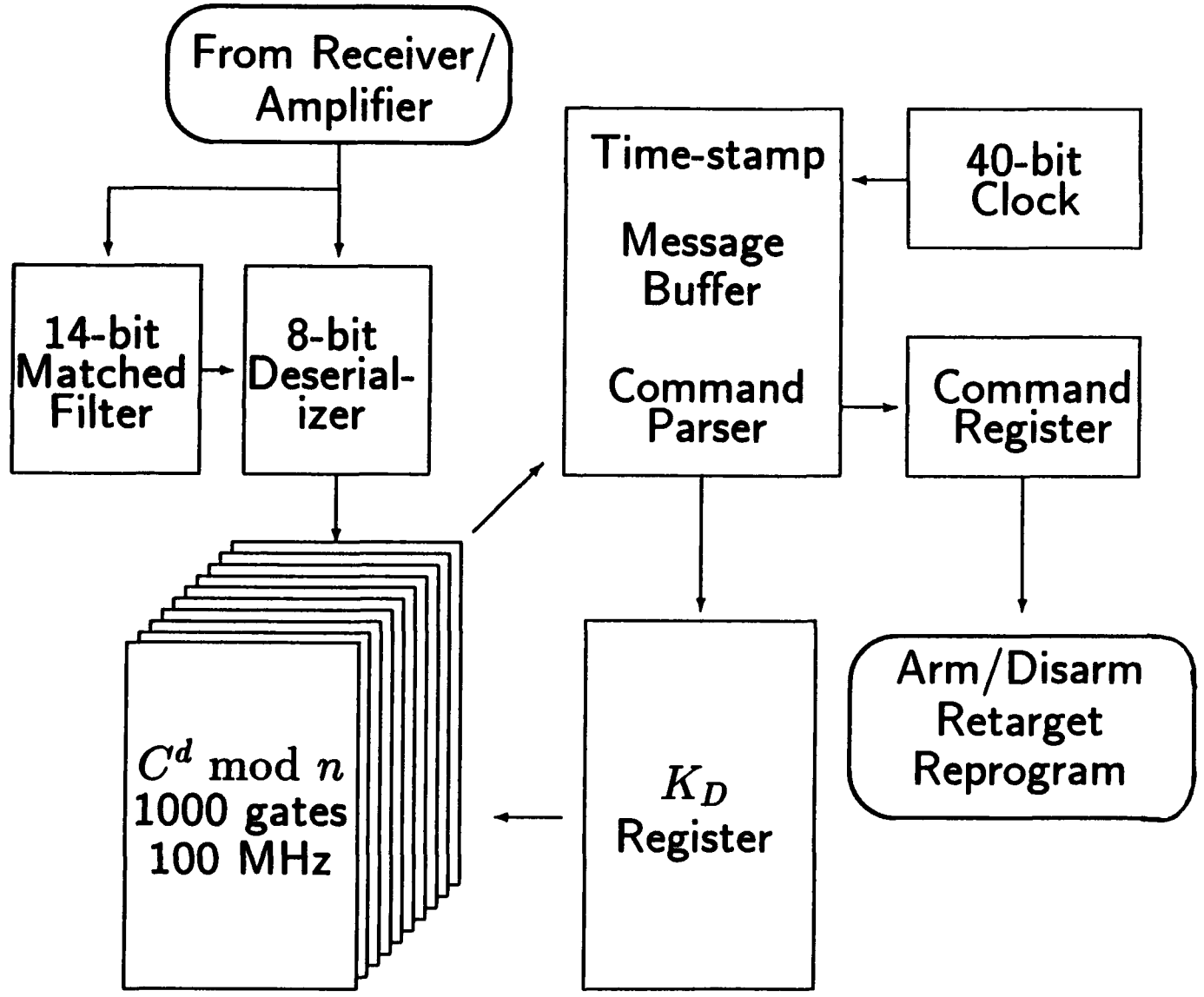
AS-IS PROCESSOR REQUIREMENTS - I

IDA
DEFENSE SCIENCE STUDY GROUP

- AS-IS RSA implementation:
  - utilize 64-bit prime numbers for NCA and AS-IS keys
  - 2^8-letter alphabet:
    $k = 7$-letter plaintext message units
    $l = 8$-letter cyphertext units
- For real-time decryption of incoming message stream:
  - perform modular exponentiation by repeated squaring and inverse residues (for signature validation) with Euclidean algorithm
  - computational work dominated by $C^d \bmod n$
  - time required is $\mathcal{O}(\ln d \cdot \ln^2 n)$

NOTIONAL AS-IS PROCESSOR

IDA
DEFENSE SCIENCE STUDY GROUP



UNCLASSIFIED

AS-IS PROCESSOR REQUIREMENTS - II

IDA
DEFENSE SCIENCE STUDY GROUP

- $\sim 10^6$ bit-ops required to decrypt each message unit
- Assume: 1000-gate module is clocked at 100 Mhz
  - $\sim 10^5$ messages per second are decrypted per module
  - SIMD design (10 signal-processor modules) with 10,000-gates keeps pace with 1 million discrete unit addresses on a one-second cycle (256 Mbit/sec bandwidth)
- ECC/parity operations performed on incoming stream with single 10,000-gate processor
- Command/Status/Keys held in 100,000-gate register array
- Control, sequencing, and 40-bit clock ops performed with a 50,000-gate module
- AS-IS digital requirements: $< 2 \times 10^5$ gates (single chip) clocked at 100 Mhz (256 Mbs data 8-way demultiplexed to 32 Mbyte/sec)
- Cross-check and vote triple redundancy straight-forward

(This page is intentionally left blank)

APPENDIX B

RED TEAM EVALUATION

ACTIVE SAFING AND ISOLATION SYSTEM (AS-IS)

RED TEAM EVALUATION

Active Safing and Isolation System (AS-IS)
RED TEAM EVALUATION

I. INTRODUCTION

On February 19, 1992, the Institute for Defense Analyses convened to discuss the concept of Active Safing and Isolation System (AS-IS). The attendees included experts from the Department of Defense, the Central Intelligence Agency, the National Security Agency, The National Defense University, and the Institute for Defense Analyses.[1] The group provided a Red Team evaluation of the AS-IS concept.

The team discussed both the technical feasibility and the possible application of AS-IS. The discussion focused primarily on the merits of AS-IS as a positive control system for naval nuclear weapons, but briefly touched on tactical applications of the system as well. The group agreed, as a baseline, to leave aside the issue of cost in any detail, but did provide some general comments about the apparent cost/benefit trade-offs of the concept.

The present authors do not necessarily agree with all of the findings of the Red Team Evaluation and believe that many are more pessimistic than warranted. For the benefit of the reader, however, a summary of the evaluation is presented here.

II. RED TEAM EVALUATION

A. Summary

Overall, the comments from the Red Team were unfavorable. While most of the team felt that the AS-IS concept could be achieved technically, they had considerable concern about the application and reliability of the system -- both in peacetime and during hostilities. As a positive control system for naval nuclear weapons, AS-IS seemed to provide little real benefit over conventional PALs. Nor did the Red Team subscribe to the use of AS-IS on tactical weapons. So, in that light, the full costs of developing the system were felt to outweigh its benefits.

---

1 Attendees included Mr. Gary Betourne (OADS/ISP/SFP); CAPT Gerald Dunne, USN (DPB); Dr. Harold Freitag (IDA/CSED); Dr. Jeffrey Grotte (IDA/SF&RD); Dr. Thomas Julian (NDU/CCRP); Dr. Steven Kramer (IDA/S&TD); Mr. Barry Levin (CIA/OSWR); Mr. William Marks (NSA/V6); Mr. John Robertson (IDA/SED); CAPT James Tisaranni, USN (DDR&E/S&TNF); Mr. Fred Wergeles (CIA/OSWR); Dr. Howard Whetzel (IDA/SED).

B. AS-IS in Brief

AS-IS deals with the ability to control a weapon once it is sold, deployed, or launched. The system began as an idea -- primarily for conventional weapons, such as the Stinger missile -- for safeguarding weapons that are sold or given to foreign countries, and might later fall into the hands of adversaries.

The concept grew into an application for the control of sea-launched ballistic missiles (SLBMs), driven by a renewed interest in the lack of an appropriate permissive-action link (PAL) for naval nuclear weapons. Those who support the AS-IS concept believe that it is a better mechanism than PALs for submarine launched weapons, primarily because of its minimal impact on the mission and operations of SLBMs: it does not divulge the location of a submarine; it does not use a complicated system of keys; it does not add to submarine launching operations; and it preserves the physical capability of the SSBN crew to launch a strike even if the strategic communication systems are destroyed.

The overall concept is a simple one. AS-IS broadcasts control messages to SLBMs via satellites, with no prior knowledge of their location. The system has global coverage and could be used to intercept an unauthorized or accidental missile launch. AS-IS relays a message to arm or disarm a missile, alter its trajectory, or deactivate a warhead, after the launched missile breaks water. *The AS-IS system, however, does not prevent a missile* from being launched. The satellites receive messages from the National Command Authority (NCA). In practice during peacetime, for example, the satellite would send continuous "disarm" messages to SLBMs. If an accidental launch occurred, the missile would be disarmed or diverted.

C. Red Team Assessment

1. PALs versus AS-IS

If a policy decision is made to employ a positive control system on SLBMs, why use AS-IS instead of existing PALs? Like other nuclear weapons, submarines receive a signal authorizing the launch of a weapon. In the past, communications to submarines were less effective than to land-based missiles. One member described how a submarine often had to piece together several messages to come up with a valid emergency action message. But communications is no longer a problem. It was explained that the same PAL message that goes to the Minuteman goes to SLBMs. On the submarine, however, the message is ignored since PALs are not part of launch procedures.

Furthermore, it was asserted that the notion of "compromising SLBM operations" -- as presented in the briefing -- is inaccurate. There are many arguments against most of the benefits ascribed to AS-IS as compared to PALs. One member went on to say that the PAL message does not compromise the "stealth" of a submarine. The PAL message is longer and harder to receive, but the message gets through. So the operational disadvantages of PALs are overstated.

Another member added that procedures already exist to prevent the launch of an SLBM: the only real use for AS-IS is against a rogue crew. And the possibility of conspiracy is very low -- crews on submarines are large and launch procedures are elaborate.

So, it was pointed out, the issue of PALs and SLBMs is less technical than operational. The Navy's biggest problem with PALs is that it hangs more bells and whistles on the missile that the Navy wants. Those same arguments apply to AS-IS.

Another problem was raised. AS-IS requires a change in operational procedures on the part of the NCA. In wartime it depends heavily on the NCA node. With AS-IS the President is responsible not only for authorizing the launch of a nuclear weapon, but also for turning off the satellite -- ensuring that the SLBMs are receiving an "enable" message. It was pointed out that, like PALs, AS-IS requires a positive action to launch a weapon. He argued that the positive action has simply been transferred from the missile site to the NCA.

A Red Team member explained that a strength of strategic systems is that once the emergency action message is received, the responsibility for launch is in the hands of the persons in the submarine or the silo, who are trained to handle the decision. AS-IS distributes critical elements of the action system to space and to the NCA. The NCA is not a place where more action and responsibility should be placed. This could confuse, slow down or degrade what is now an orderly process. If an emergency action message gets garbled in the current system, the worst outcome is that the missile does not get fired. With AS-IS mistakes could be more costly, the whole system could be destroyed.

In addition, it was suggested that AS-IS could lower confidence on board the submarine by raising the uncertainty as to whether weapons will really work when they need to. With AS-IS, part of the control lies outside the system, which introduces vulnerability. By contrast, a PALs system has work arounds that have been learned over long periods of time, in case of failure. It was added that AS-IS takes away some of the commanding officer's responsibility. AS-IS could increase the probability that a weapon

would be launched in a situation where there is doubt or confusing signals. Now there is no safety net for mistakes -- which means more control.

Given the experience and infrastructure in place to support PALs, it seems to be a simpler solution to the need for a control system for SLBMs. AS-IS, by contrast, would require a whole new set of procedures, training, and infrastructure. Moreover, as it was pointed out, the easiest PAL is the emergency action message itself. If a second message is introduced -- AS-IS -- it gives the enemy a second opportunity to disrupt communications.

It was argued that positive control of naval nuclear weapons is a small problem. As an "assure against" device, AS-IS seems flawed and may in fact offer little improvement over the level to which weapons are now controlled. In addition, a more effective missile control device should provide control before a missile is launched. It is toward that sort of system that resources should be devoted. For now, PALs are a far less expensive alternative.

2. Exploiting AS-IS

a. Tamper-proofing and reliability

One member raised the question of tamper-proofing, or as another suggested tamper-resistance. Several members agreed that any system put on a missile can be beaten by technicians, or could lead to a less reliable missile. Beating the lab guys is very difficult. So a conspiracy could occur with or without the system.

And while the Red Team generally agreed that tamper-resistant attributes could be added to the system, it was explained that the tradeoff in reliability is unacceptable to the Navy. In a submarine force, the system is simple. Simplicity and experience lead to reliability. And nothing at sea is new, the systems have evolved. The D-5, for example, does not have that much new technology. AS-IS adds complexity to the rocket. It is not simply a matter of adding a chip or two: it means adding a receiver, a crypto system, antennae, tamper resistance, etc. Equipment fails. Adding more equipment reduces reliability.

Moreover, the information presented in the briefing makes it difficult to evaluate how reliable AS-IS is. It was pointed out that there is a difference between the functionality of a chip and an end-to-end process. The system adds complexity and increases the number of failure modes. What is the probability of failure; how many

failures are possible; at what frequency? This information is critical to evaluating the system.

It was noted that everything on a missile, now, is required. Reliability tests will be the Achilles heel for this program. Adding something else increases the failure rate and introduces a new element into the critical path. For example, adding leads into a guidance assembly is a very weak link. Onboard a submarine, crews have access to the leads, increasing the probability of compromise. It was added that the antennae can be disrupted by bad weather, water, or any number of other factors. So, it reduces the capability to shut down a missile with 100 percent reliability. It was suggested that the failure rate and reliability of AS-IS needs to be more explicit and then compared with some other form of PALs, to calibrate its value.

b. Single-Point to Failure

It was argued that a significant weakness of the system is its single point to failure -- a point design system -- that can lead to problems, whether it be through tampering or satellite transmission. This sort of system provides incentives to others to find the point to failure and cut it off. The strategic triad, with its land, sea, and air based legs, was designed to avoid a single point of failure. And in each system there have been failures, so the concept of the triad is very important.

c. The Satellite Link

A question was raised concerning satellite disruption. How far can satellite performance be degraded and the system still function? What is the performance margin of the satellite? And while the system is conceived primarily to prevent an unauthorized launch during peacetime, it is still necessary to consider the case of hostilities. Arguably during hostilities, absolute control over weapons is more important than during peacetime.

The system seems quite vulnerable to jamming or to overload by continuous broadcasting -- an action that an adversary might take to disrupt the system. It was argued that over time an adversary can determine the power, sequence, and frequency of the AS-IS message and can jam the system with noise. Once the system is defeated, positive control is lost. If an adversary can demonstrate loss of control, the value of the system is degraded and the NCA's confidence in controlling weapons is undermined. The system is not an end game. And the scenario, while political, is a realistic one.

Moreover, the argument that if the satellite fails, the situation reverts to the "status quo" is flawed. The default mode of the system is overemphasized. A positive control system is implemented in response to a need. Once implemented, the "status quo" changes. So if the system fails or is disrupted, positive control is lost; it is impossible to return to the previous status quo.

It was added that if the United States thought that the former Soviet Union had a similar system, the United States would be willing to spend a lot of money trying to exploit it. Furthermore, it seems hard to imagine that the President would actually allow AS-IS to be included in a package of shared (i.e., multinational) control.

3. Launch Detection

The question of launch detection was raised. Since the system does not intercept the missile until after breakwater, it is possible that the launch might be detected. If so, it creates uncertainly that could lead to false retaliation. If the system does not prevent launch, it does not buy enough. It was argued that it is most likely that the missile will not be intercepted until after the first stage motor launch, increasing the probability of the being launch being detected by others.

4. *Operational Concerns*

Several operational issues were raised.

- How are operational tests performed? If AS-IS is embedded in existing circuitry, the circuitry needs to be tested after routine maintenance. It was added that to adequately test the system, realistic messages need to be generated. How can the system be tested and replaced securely?
- What about the need to fire a missile, on short notice, because of an accident or fire?
- How can AS-IS address individual missiles when the targeting is not predetermined? The ability to separately address individual weapons is an interesting attribute of AS-IS, not available within the current system. But missiles are located in one of 24 tubes, the targeting of which is not predetermined. So the tube-to-target relationship can be changed at any time. The NCA would not know the missile patch, and therefore which missile to disarm. It would, in theory, be very interesting to be able to turn off all missiles targeted at Moscow, but without the missile patch, how would this be operationally possible?

A further complexity was added. Submarines rotate as well as missiles. So target packages shift not only among missiles, but also among ships. Turning off a specific missile seems technically possible, but how the system knows whether it is the right missile is in question.

5. System Security

The issue of security was raised. When eight satellites transmit 24 hours a day, security is an issue -- far more so than with a system that transmits less frequently. As a result, AS-IS has the potential to be less secure that the system in place today.

One member also cautioned about the use of public and private keys with respect to system security. While it might be interesting to explore the use of a public/private system, it has drawbacks. It was added that public/private keys are not sufficiently secure. Having part of the message publicly available simplifies decryption. So the system needs a proven, secure key.

It was argued that time stamps may also lower security. The time stamp introduces a commonalty between messages. And it changes in a predetermined manner, so the messages are not entirely independent. These aspects add a "hook" that can facilitate decryption.

6. Tactical and Other Applications

Few members of the Red Team supported the use of AS-IS for tactical applications, except for the possibility of very limited applications. It was pointed out that the system imposes an additional burden on potential buyers that would make U.S. weapons very unattractive. Furthermore, there is the problem of accounting for weapons -- knowing where systems are and figuring out which systems to enable or disable. The world is very complex and the problem is not a simple one.

Important also are the political costs of tactical applications. If the United States puts AS-IS on tactical weapons that are sold abroad, it implies some level of responsibility on the part of the United States over the use of the weapons. If the weapons are used or there is an accident, the United States becomes the responsible actor, at least in part -- for not having the system disabled -- rather than whoever had control of the weapon. The United States is effectively inserted into any conflict in which the weapons are used.

Several operational problems that might arise during hostilities were also raised. Cellular transmitters that send the signal to tactical weapons can be easily shot down,

rendering them unable to transmit an "enable" message to the weapons. It is a single point to failure: if the transmitters are knocked out, the weapon is knocked out. And even if the system can be "locked" into enable status, it is one additional requirement for the infantry during high stress situations. Things go wrong all the time; the most common mistake is to forget the batteries for the radio. So the system inserts doubt into the mind of an infantry person -- already being asked to do a very difficult job -- as to whether the weapon will fire when needed. Moreover, "enabled" weapons can still, during conflict, get into the hands of the enemy and be used.

Some member of the Red Team did raise limited applications of AS-IS. It was suggested that tactical applications may offer an opportunity for covert emplacement. It was noted that AS-IS technology may have applications in conjunction with new satellite capabilities that will enable a few satellites to communicate throughout the world. Or, as was also mentioned, AS-IS type technology might be used with GPS to control activity in a given region of the world. One member noted that the concept has merit as a remote satellite launching system, with possible use in broader applications. Another member added the use of AS-IS for IFF, or perhaps with high-value commercial products.

7. Cost

While cost was not a central theme, many members of the Red Team cautioned against expressing costs in hardware terms only. A more realistic assessment of cost must include the range of system development and maintenance costs -- development, testing, evaluation, training, infrastructure, hardware, operational maintenance, and support. And these costs need to be compared to other alternatives, namely existing PAL systems or taking no action at all, in order to be credible.

As one member noted, controlling SLBMs is a low level problem, for now. A simple, elegant, low-cost system is needed. AS-IS is not that. So it is hard to support the system from a policy perspective. Furthermore, it was pointed out that it does not seem useful to add high costs to solve a peacetime problem with a method that might prove to be worrisome during hostilities.

8. Other Comments

a. Bandwidth

The group spent some time discussing bandwidth. One member noted that the bandwidth for AS-IS was greater than for ELF. It was also suggested that the AS-IS

concept might have a communication advantage over ELF, in that a more complicated message can be sent than through ELF. But concern was expressed over the practical throughput needs of the system. Transmission rates for AS-IS will be high, so it may be difficult to get the needed bandwidth.

b. Error Rates

During the discussion of bit error rates for digital coding schemes, it was suggested that the error rates be compared to the current NAVSAT system. Unless the signal is stronger than NAVSAT, it will not get through. The comparison provides a useful frame of reference for evaluation.

It was also mentioned that clock synchronization has long been a difficult problem in communications.

III. SUMMARY OF AUTHORS' VIEWS

Most of the Red Team discussions dealt with the relative merits of the existing PAL controls over the proposed AS-IS concept. There was uniform agreement that, if the communications required in the PAL system currently in place for controlling Air Force nuclear missiles are deemed reliable enough for submarine application, then that system is clearly the simpler and more cost-effective solution. In fact, AS-IS was proposed solely to deal with the scenario in which the existing PAL is assumed to be insufficiently reliable for SLBM use. Under the existing PAL, the emergency action message must successfully reach the launch site -- presumably under electronic warfare conditions -- in order for the missile to be launched. Under the AS-IS proposal, communications must reach the missile only during peacetime, when DISABLE signals are being transmitted by the NCA. During wartime, when communications are less reliable, no communication with the missile is needed to permit launch.

There was general agreement that, on technical grounds alone, the AS-IS concept appears to be feasible. Certain operational issues raised by the Red Team do warrant serious consideration. However, the key issue on which further consideration of AS-IS hinges is the suitability of the current PAL controls. If the present PAL system is considered insufficiently reliable for SLBM use, the AS-IS concept may warrant further study.

APPENDIX C

DISTRIBUTION LIST

DISTRIBUTION LIST
FOR IDA PAPER P-2783

Office of the Secretary of Defense	Number of Copies
The Honorable Victor H. Reis Director Defense Research and Engineering The Pentagon, Room 3E1014 Washington, D.C. 20301	1
The Honorable Robert C. Duncan Director, OT&E The Pentagon, Room 3E318 Washington, D.C. 20301	1
Defense Science Board The Pentagon, Room 3D865 Washington, D.C. 20301	
Dr. John Foster, Chairman	1
Mr. John V. Ello, Executive Director	1
Mr. Franklin C. Miller Deputy Assistant Secretary Nuclear Forces and Arms Control Policy, OASD(ISP) The Pentagon, Room 4C762 Washington, D.C. 20301	1
U.S. Nuclear Command and Control System Support Staff Skyline #3, Suite 500 5201 Leesburg Pike Falls Church, VA 22041	
Captain O.D. Scarborough, III, USN	1
Colonel Randy Blanks, Chairman, Fail Safe & Risk Reduction Study	1
Defense Advanced Research Projects Agency 3701 N. Fairfax Dr. Arlington, VA 22203-1714	
Dr. Gary L. Denman, Director	1
Dr. Ira Skurnick, DSO	1
Major General Malcolm O'Neill, USA Deputy Director SDIO The Pentagon, Room 1E801 Washington, D.C. 20301	1
Colonel Robert Hughes, USAF National War College Ft. Lesley J. McNair Washington, D.C. 20319	1

Mr. Gary P. Betourne
Strategic Forces Policy
OASD/International Security Policy 1
The Pentagon, Room 4B880
Washington, D.C. 20301-2600

Captain Gerald Dunne, USN
Executive Director
Defense Policy Board 1
The Pentagon, Room 4B947
Washington, D.C. 20301

Dr. Thomas Julian
INSS/ORS/CCRP
National Defense University 1
Ft. Lesley J. McNair
Washington, D.C. 20319

Captain James Tisaranni, USN
Missiles and Space Systems 1
OUSD (A)/S &SS
The Pentagon, Room 3E129
Washington, D.C. 20301

U.S. Government

Mr. Thomas Garwin
House Armed Service Committee
Rayburn Bldg. 2120 1
U.S. Congress
Washington, D.C. 20515

Mr. John Mansfield
Committee on Armed Services
232A Russell Senate Office Bldg. 1
Capitol Complex
Washington, D.C. 20515

Mr. William Hoehn
Senate Armed Service Committee 1
228 Senate Russell
Washington, D.C. 20510

Mr. David Hafemeister
Senate Foreign Relations Committee
Senator Dirksen Office Bldg., Room 446 1
U.S. Senate
Washington, D.C. 20510

U.S. Arms Control and Disarmament Agency
Washington, D.C. 20451
Ambassador Linton Brooks 1
Dr. Barbara A.B. Seiders, Chief of Research, Office of Chief Science Advisor 1

Mr. Robert G. Bradley
Advanced Command and Control 1
Sandia National Laboratories
Albuquerque, NM 87185-5800

Ms. Patricia Minard
1144 Wimbledon Dr. 1
McLean, VA 22101

U.S. Department of Commerce
Washington, D.C. 20230
Mr. John A. Richards, Deputy Assistant Secretary, Industrial Resource Administration 1

Office of Technology Assessment/ISC
U.S. Congress
Washington, D.C. 20510-8025
Dr. Thomas Karas 1
Dr. M. Anthony Fainberg 1

Captain Jim Wilson, USN
Naval Studies Board
National Research Council 1
2101 Constitution Ave., N.W.
Washington, D.C. 20418

Mr. Barry Leven
OSWR
Central Intelligence Agency 1
Washington, D.C. 20505

Mr. William Marks, V6
National Security Agency 1
9800 Savage Road
Ft. George G. Meade. MD 20755-6000

Defense Technical Information Center
Cameron Station 1
Alexandria, VA 22314

Mr. Fred Wergeles
OSWR
Central Intelligence Agency 1
Washington, D.C. 20505

Other

Admiral Robert J. Long, USN (Ret.)
247 Hearman's Way 1
Annapolis, MD 21401

VADM Daniel L. Cooper
Gilbert Commonwealth 1
P.O. Box 1498
Reading, PA 19603

Dr. Richard L. Garwin
IBM Fellow 1
Thomas J. Watson Research Center
Yorktown Heights, NY 10598

The RAND Corporation
P.O. Box 2138
Santa Monica, CA 90406-2138
Mr. Dean Wilkining, Director, Force Employment 1
Mr. Bruce Hoffman, Terrorist and Counterterrorist Analyst 1

Dr. Ashton Carter
Center for Science and International Affairs
J.F. Kennedy School of Government 1
Harvard University
79 John F. Kennedy Street
Cambridge, MA 02138

Institute for Defense Analyses 40
1801 N. Beauregard St.
Alexandria, VA 22311-1772

Defense Science Study Group

Professor Daniel Alpert
Director, Program in Science, Technology and Society 1
University of Illinois
912-1/2 West Illinois
Urbana, IL 61801

Professor R. Stephen Berry
Department of Chemistry
University of Chicago 1
5735 South Ellis Avenue
Chicago, IL 60637

Dr. Solomon J. Buchsbaum
Senior Vice President
Technology Systems, 3L-650 1
AT&T Bell Laboratories
Holmdel, NJ 07733-1988

Professor Stephen P. Boyd
111 Durand
Electrical Engineering Department
Stanford University
Stanford, CA 94305 — 1

Professor Russel Caflisch
Department of Mathematics
University of California
405 Hilgard Avenue, MA-01
Los Angeles, CA 90024-1555 — 1

Professor Stephen A. Campbell
Department of Electrical Engineering
University of Minnesota
200 Union Street, S.E.
Minneapolis, MN 55455
(612) 625-5876
FAX: (612) 625-4583 — 1

Professor Steven K. Case
CyberOptics Corporation
2331 University Avenue, SE
Minneapolis, MN 55414 — 1

Professor Vicki L. Chandler
Institute of Molecular Biology
University of Oregon
Eugene, OR 97403 — 1

Professor Peter Chen
Department of Chemistry
Harvard University
12 Oxford Street
Cambridge, MA 02138 — 1

Dr. Susan N. Coppersmith
AT&T Bell Laboratories
1D351
600 Mountain Avenue
Murray Hill, NJ 07974 — 1

Dr. Werner J. A. Dahm
Department of Aerospace Engineering
University of Michigan
Ann Arbor, MI 48109-2140 — 1

Professor William J. Dally
Artificial Intelligence Laboratory
Massachusetts Institute of Technology
545 Technology Square
Cambridge, MA 02139 — 1

Professor Mark E. Davis
Chemical Engineering 210-41
California Institute of Technology
Pasadena, CA 91125 — 1

Professor Robert H. Davis
Department of Chemical Engineering
University of Colorado
Boulder, CO 80309-0424 — 1

Dr. Ruth Davis
President
The Pymatuning Group, Inc.
4900 Seminary Road
Suite 570
Alexandria, VA 22311 — 1

General Russell E. Dougherty, USAF (Ret.)
2359 S. Queen Street
Arlington, VA 22202 — 1

Professor Katherine T. Faber
Department of Materials Science and Engineering
Northwestern University
The Technological Institute
Evanston, IL 60201 — 1

Dr. Alexander H. Flax
National Academy of Engineering
2101 Constitution Ave., N.W.
Room 306
Washington, D.C. — 1

Professor Joseph S. Francisco
Department of Chemistry
Room 33
Wayne State University
Detroit, MI 48202 — 1

Professor S. James Gates, Jr.
Department of Physics and Astronomy
Howard University
Washington, D.C. 20059 — 1

Professor Steven M. George
Department of Chemistry and Biochemistry
Campus Box 215
University of Colorado
Boulder, CO 80309-0215 — 1

General A. J. Goodpaster, USA (Ret.)
409 North Fairfax Street
Alexandria, VA 22314 — 1

General Paul F. Gorman, USA (Ret.)
Cardinal Point, Inc.
Route 1, Box 352
Afton, VA 22920 — 1

Professor Nancy M. Haegel
Department of Materials Science and Engineering
5731 Boelter Hall
University of California
Los Angeles, CA 90024 — 1

Professor Bruce Hajek
University of Illinois
1101 West Springfield, CSL
Urbana, IL 61801 — 1

Professor Thomas C. Halsey
The James Franck Institute
University of Chicago
5640 South Ellis Avenue
Chicago, IL 60637 — 1

Professor James M. Howe
Department of Materials Science
Thornton Hall
University of Virginia
Charlottesville, VA 22903 — 1

Professor Robert A. Hummel
Courant Institute of Mathematical Sciences
New York University
251 Mercer Street
New York, New York 10012 — 1

Professor Deborah A. Joseph
Computer Sciences Department
University of Wisconsin
1210 W. Dayton Street
Madison, WI 53706 — 1

Professor Randy H. Katz
Computer Science Division
Department of Electrical Engineering
University of California
Berkeley, CA 94720 — 1

Admiral Isaac C. Kidd, USN (Ret.)
6287 Chaucer View Circle
Alexandria, VA 22304 — 1

Professor Steven E. Koonin
W.K. Kellogg Radiation
Laboratory 106-38 — 1
California Institute of Technology
Pasadena, CA 91125

Dr. Martha Krebs
Associate Director
Planning & Development — 1
Lawrence Berkeley Laboratory
Berkeley, CA 94720

Professor Frederick K. Lamb
Department of Physics
University of Illinois — 1
1110 West Green Street
Urbana, IL 61801

Professor Kevin K. Lehmann
Frick Chemical Laboratories
Princeton University — 1
Washington Road
Princeton, NJ 08544-1009

Professor Nathan S. Lewis
Mail Code 127-72
Chemistry Department — 1
California Institute of Technology
Pasadena, CA 91125

Professor Philip S. Marcus
Department of Mechanical Engineering — 1
University of California
Berkeley, CA 94720

Professor David L. McDowell
The George W. Woodruff School of Mechanical Engineering — 1
Georgia Institute of Technology
Atlanta, GA 30332-0325

Professor Anne B. Myers
Department of Chemistry — 1
University of Rochester
Rochester, NY 14627

Professor Gerald A. Navratil
Department of Applied Physics
Columbia University — 1
215 S.W. Mudd Building
New York, NY 10027

Dr. Daniel M. Nosenchuck
Department of Mechanical
and Aerospace Engineering
Princeton University
Princeton, NJ 08544-5263 — 1

Professor Robert A. Pascal, Jr.
Frick Chemical Laboratory
Princeton University
Washington Road
Princeton, NJ 08544-1009 — 1

Professor Anthony T. Patera
Room 3-264
Department of Mechnical Engineering
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139 — 1

Professor S. S. Penner
University of California, San Diego
Center for Energy and
Combustion Research, B-010
La Jolla, CA 92093 — 1

Professor David Pines
University of Illinois
Department of Physics
Loomis Laboratory of Physics
1110 West Green Street
Urbana, IL 61801 — 1

Professor Dennis L. Polla
Department of Electrical Engineering
University of Minnesota
200 Union Street, SE
Minneapolis, Minnesota 55455 — 1

Professor Thomas A. Prince
220-47
Division of Physics, Mathematics and Astronomy
California Institute of Technology
Pasadena, CA 91125 — 1

Professor Thomas F. Rosenbaum
James Franck Institute
University of Chicago
5640 Ellis Avenue
Chicago, IL 60637 — 1

Professor Stephen W. Semmes
Department of Mathematics
Rice University
P.O. Box 1892
Houston, TX 77251 — 1

Professor Steven J. Sibener
James Franck Institute
University of Chicago
5640 Ellis Avenue
Chicago, IL 60637 — 1

Professor Theodore A. Slaman
Department of Mathematics
University of Chicago
5734 University Avenue
Chicago, IL 60637 — 1

Professor Daniel L. Stein
Department of Physics
University of Arizona, Bldg. 81
Tucson, AZ 85721 — 1

Admiral Harry D. Train, III, USN (Ret.)
100 West Plume Street
Suite 313
Norfolk, VA 23510 — 1

Professor Peter W. Voorhees
Department of Materials Science and Engineering
Northwestern University
Evanston, IL 60208 — 1

Professor Warren S. Warren
Department of Chemistry
Princeton University
Princeton, NJ 08544 — 1

Professor Robert L. Whetten
Department of Chemistry and Biochemistry
University of California
Los Angeles, CA 90024-1569 — 1

Professor R. Stanley Williams
Department of Chemistry and Biochemistry
405 Hilgard Avenue, CH-01
University of California
Los Angeles, CA 90024-1569 — 1

Professor W. Hugh Woodin
Department of Mathematics
Evans Hall
University of California
Berkeley, CA 94720 — 1

Professor Herbert York Director, Science, Technology and Public Affairs, Q-060 University of California, San Diego La Jolla, CA 92093	1
Total Distribution	**136**

(This page is intentionally left blank)